มาตรการทางกฎหมายที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

นางสาว สุธาสินี พรหมมินทร์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2545

ISBN 974-17-3315-1

CRIMINAL MEASURES AGAINST CRIME IN ELECTRONIC FUND TRANSFERS

Miss Sutasinee Prommintar

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Laws in Laws
Faculty of Law
Chulalongkorn University
Academic Year 2002

ISBN 974-17-3315-1

หัวข้อวิทยานิพนธ์	มาตรการทางกฎหมายที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์
โดย	นางสาวสุธาสินี พรหมมินทร์
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ วีระพงษ์ บุญโญภาส
อาจารย์ที่ปรึกษาร่วม	ผู้ช่วยศาสตราจารย์ อิทธิพล ศรีเสาวลักษณ์

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะนิติศาสตร์
(ผู้ช่วยศาสตราจารย์ ชิติพันธุ์ เชื้อบุญชัย)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.อภิรัตน์ เพ็ชรศิริ)

..... อาจารย์ที่ปรึกษา
(รองศาสตราจารย์ วีระพงษ์ บุญโญภาส)

..... อาจารย์ที่ปรึกษาร่วม
(ผู้ช่วยศาสตราจารย์ อิทธิพล ศรีเสาวลักษณ์)

..... กรรมการ
(อาจารย์สุทธิชัย จิตรวาณิช)

..... กรรมการ
(ดร.ทวีศักดิ์ กออนันตกูล)

สุธาสินี พรหมมินทร์ : มาตรการทางกฎหมายที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ (CRIMINAL MEASURES AGAINST CRIME IN ELECTRONIC FUND TRANSFER) อ. ที่ปรึกษา: รศ.วีระพงษ์ บุญโญภาส, อ.ที่ปรึกษาร่วม: ผศ.อิทธิพล ศรีเสาวรักษ์ จำนวนหน้า 335 หน้า . ISBN 974-17-3315-1

"อาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์" เป็นการกระทำความผิดในการกระทำการทุจริตต่อระบบโอนเงินทางอิเล็กทรอนิกส์ หรือการทุจริตต่อระบบคอมพิวเตอร์ รวมถึงอุปกรณ์อิเล็กทรอนิกส์ ไม่ว่าจะเป็นการฉ้อโกงบัตรเครดิต บัตรเดบิต หรือบัตรพลาสติกอื่นๆ หรือการฉ้อโกงคอมพิวเตอร์ ซึ่งการกระทำดังกล่าวอาจเป็นการกระทำในฐานความผิดเกี่ยวกับ "การเข้าถึงข้อมูลทางอิเล็กทรอนิกส์" หรือ "การเข้าถึงโดยปราศจากอำนาจ" นอกจากนั้นอาชญากรรมดังกล่าวได้รวมถึงการกระทำความผิดต่อการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์โดยถือว่าเป็นความผิดที่ใช้การโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิด เพื่อปิดบังที่มาที่แท้จริงของเงินหรือทรัพย์สินที่รวมอยู่ในการโอนเงินผ่านการโอนเงินทางอิเล็กทรอนิกส์ ประกอบกับการให้บริการทางธนาคารในการโอนเงินทางอิเล็กทรอนิกส์ถือว่าเป็นข้อมูลเฉพาะบุคคล ที่อยู่ หมายเลขบัญชี หรือรายการทางบัญชีซึ่งจัดเป็นข้อมูลลับทางธนาคารที่ไม่อาจเปิดเผยต่อบุคคลทั่วไปได้ และเทคโนโลยีทางด้านคอมพิวเตอร์ในการอำนวยความสะดวกแก่การโอนเงินทางอิเล็กทรอนิกส์ในปัจจุบันสามารถกระทำได้โดยสะดวกและรวดเร็ว

วิทยานิพนธ์ฉบับนี้ผู้เขียนได้เสนอแนะแนวทางในการกำหนดกฎหมายโอนเงินทางอิเล็กทรอนิกส์และการกำหนดบทลงโทษอันเป็นการคุ้มครองบุคคล รวมถึงแนวทางในการเยียวยาความเสียหายที่เกิดขึ้นจากอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ เพื่อนำแนวทางดังกล่าว มาพัฒนากฎหมายของประเทศให้สามารถบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าวได้อย่างมีประสิทธิภาพ

สาขาวิชา นิติศาสตร์ ลายมือชื่อนิสิต.....

ปีการศึกษา 2545 ลายมือชื่ออาจารย์ที่ปรึกษา.....

ลายมือชื่ออาจารย์ที่ปรึกษาร่วม.....

4286141334 : MAJOR LAWS
KEY WORD: / / / /

SUTASINEE PROMMINTAR : CRIMINAL MEASURES AGAINST CRIME IN ELECTRONIC FUND TRANSFERS. THESIS ADVISOR: ASSOC.PROF.VEERAPHONG BOONYOPHAS, THESIS COADVISOR : ASST.PROF.EATHIPOL SRISAWALUCK ,335 pp. ISBN 974-17-3315-1

"Crime in Electronic Fund Transfers" is the term of descriptive of offence involving conduct dishonest of electronic fund transfer system, untruthful of computer system including access device fraud, credit card fraud, debit card fraud, debit card fraud or plastic card fraud or computer fraud in fund transfer. These conduct is act by access device or unauthorized access device and else offence to use transfer fund to conceal or disguise nature of money or property believed to be the proceeds of unlawful activity or derive from serious crime which is held that crime of electronic fund transfers. In addition, The transfers of money is held that identification of person, address, account, transaction is secrecy of bank, which is disclose. And the rapid advancement in the field of computer and technology of transfer of money or funds or account transaction that it facilitates money launder of offender conduct electronic fund transfers crime increase speedily.

This Thesis suggests appropriate approaches for prevent, control, supervising, discontinue, penalty of offences or crimes in electronic fund transfers and remedy measure of damage from proceeds of serious crime which given that appropriate approaches to estimate measures against or enforcement of offences or crimes in electronic fund transfers.

Field of study Laws
Academic year 2002

Student's signature Sutasinee Prommintar
Advisor's signature V. Boonyophas
Co-advisor's signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จลุล่วงไปด้วยดี เนื่องด้วยความเมตตาของท่านคณาจารย์ผู้มีพระคุณทั้งหลายที่ให้ความกรุณาช่วยเหลือและแนะนำในการจัดทำวิทยานิพนธ์ตลอดมา ผู้เขียนขอกราบขอบพระคุณท่าน รองศาสตราจารย์วีระพงษ์ บุญโญภาส อาจารย์ที่ปรึกษา ที่สละเวลาเป็นอาจารย์ที่ปรึกษาและกรุณาแนะนำแนวความคิดและสนับสนุนโครงร่างวิทยานิพนธ์นี้แต่แรกเริ่มตลอดจนได้กรุณาตรวจทานแก้ไขจนสำเร็จ และต้องขอกราบขอบพระคุณท่านผู้ช่วยศาสตราจารย์อิทธิพล ศรีเสาวลักษณ์ อาจารย์ที่ปรึกษาร่วม ที่กรุณาสละเวลามาเป็นอาจารย์ที่ปรึกษาร่วม และให้คำแนะนำและแนวทางในการเขียนและการศึกษา ตลอดจนตรวจทานแก้ไขวิทยานิพนธ์จนสำเร็จ ผู้เขียนขอกราบขอบพระคุณท่าน รองศาสตราจารย์ ดร.อภิรัตน์ เพ็ชรศิริ เป็นอย่างสูงที่กรุณาให้คำแนะนำและแนวทางในการศึกษาวิทยานิพนธ์ ตลอดจนสละเวลามาเป็นประธานกรรมการสอบวิทยานิพนธ์ และกราบขอบพระคุณท่าน อาจารย์ สุทธิชัย จิตรวาณิช และ ท่าน ดร.ทวีศักดิ์ กออนันตกูล ที่กรุณาสละเวลาอันมีค่าของท่านมาเป็นกรรมการสอบวิทยานิพนธ์ และกรุณาให้คำแนะนำต่าง ๆ ในการเขียนวิทยานิพนธ์ฉบับนี้ ทั้งนี้ ผู้เขียนขอกราบขอบพระคุณบูรพาคณาจารย์ทางนิติศาสตร์ทุกท่านที่ได้ศึกษาวิจัยและพัฒนางานทางด้านนิติศาสตร์ไว้ให้ชนรุ่นหลังได้ศึกษา รวมทั้งกราบขอบพระคุณเจ้าของวิทยานิพนธ์ทุก ๆ ท่านที่ผู้เขียนได้ศึกษาและได้อ้างอิงในการทำวิทยานิพนธ์ครั้งนี้

ผู้เขียนขอกราบขอบพระคุณ ร้อยตำรวจเอก อนุชา รัศมี ที่กรุณาให้การสนับสนุนข้อมูล และคุณสุรางคนา แก้วจำนงค์ ที่กรุณาตรวจและให้คำแนะนำต่าง ๆ ซึ่งเป็นประโยชน์อย่างมากต่อการเขียนวิทยานิพนธ์ และที่สำคัญสูงสุดผู้เขียนขอกราบขอบพระคุณอย่างสูงแก่ บิดา และ มารดาผู้มีพระคุณสูงสุด ซึ่งให้ความช่วยเหลือ สนับสนุนในทุกๆ ด้านแก่ผู้เขียนตลอดมาจนวิทยานิพนธ์เล่มนี้ได้สำเร็จลุล่วงไปด้วยนี้ อีกทั้ง ผู้เขียนขอขอบคุณ คุณประภัสรา พรหมมินทร์ ผู้ซึ่งให้ความช่วยเหลือและสนับสนุนในทุกๆ ด้าน รวมทั้งเป็นกำลังใจให้แก่ผู้เขียนเป็นอย่างมากตลอดมา และขอขอบคุณ คุณปราณี อึ่งประเสริฐ และ คุณรุจิกร ไพรินทร์ ผู้ซึ่งให้การสนับสนุน และช่วยเหลือแก่ผู้เขียน และเป็นกำลังใจแก่ ผู้เขียน รวมถึงพี่ ๆ น้อง ๆ และเพื่อนๆ ทุก ๆ ท่านที่ไม่อาจกล่าวได้หมด ณ ที่นี้ ที่ให้การสนับสนุนและเป็นกำลังใจให้แก่ผู้เขียนในการศึกษาเสมอมา

หากวิทยานิพนธ์ของผู้เขียนมีคุณค่าและมีประโยชน์ในด้านการศึกษาอยู่บ้าง ผู้เขียนขอกราบเป็นกตเวทิตาแก่ทุก ๆ ท่านที่เอ่ยนามมาข้างต้น หากมีข้อผิดพลาดประการใด ผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

สุธาสินี พรหมมินทร์

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญ(ต่อ)

หน้า

บทที่ 1

บทนำ

1.1. ความเป็นมาและความสำคัญของปัญหา

เนื่องจากภาคการเงินการธนาคารนั้น มีความสำคัญอย่างมากต่อระบบเศรษฐกิจ และสามารถสร้างความเปลี่ยนแปลงแก่สถานภาพความมั่นคงภายในประเทศและประชาคมโลก อีกทั้งระบบการเงินการธนาคารยังมีความเกี่ยวข้องต่อการดำรงชีวิต ธุรกรรมเชิงพาณิชย์ประเภทต่างๆ และการโอนหรือการเคลื่อนย้ายเงินภายใต้ระบบการเงินการธนาคาร โดยระบบการเงินการธนาคารของประเทศไทยได้มีการพัฒนาทางด้านเทคโนโลยีให้มีความสะดวกและรวดเร็ว ด้วยการนำเทคโนโลยีทางอิเล็กทรอนิกส์หรือ Electronic Banking System มาให้บริการทางการเงินอันเป็นการให้บริการผ่านสื่อกลางทางอิเล็กทรอนิกส์ ส่งผลทำให้ธุรกรรมเชิงพาณิชย์หรือการโอนหรือการเคลื่อนย้ายเงินภายใต้ระบบการเงินการธนาคารสามารถกระทำได้อย่างสะดวก ถูกต้อง รวดเร็ว นอกจากนั้นระบบอิเล็กทรอนิกส์ยังสามารถเชื่อมโยงเครือข่ายการเงินการธนาคารได้ทั่วโลก เช่น เครือข่ายอินเตอร์เน็ท เครือข่ายองค์กรความร่วมมือระหว่างประเทศ เป็นต้น

ในลักษณะเดียวกัน อาชญากรรมที่เกิดขึ้นในระบบธนาคารอิเล็กทรอนิกส์ก็สามารถสร้างความเสียหายต่อระบบการเงินการธนาคารได้อย่างมหาศาล โดยเฉพาะอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์นั้น จัดเป็นอาชญากรรมที่สร้างความเสียหายต่อระบบเศรษฐกิจของประเทศและสังคมโดยรวมได้อย่างคาดไม่ถึง โดยการกระทำความผิดดังกล่าวจะมีลักษณะที่ซับซ้อน แนบเนียน และอาศัยความทันสมัยทางด้านเทคโนโลยีคอมพิวเตอร์ในการกระทำต่อกระบวนการโอนเงินทางอิเล็กทรอนิกส์ หรือใช้กระบวนการโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการประกอบอาชญากรรม ดังนั้นอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์จะมีความแตกต่างจากอาชญากรรมโดยทั่วไป ๆ อย่างสิ้นเชิง โดยผลตอบแทนจากการกระทำอาชญากรรมประเภทนี้ก็มีมูลค่าสูง และสร้างความเสียหายทางการเงินต่อระบบการเงินการธนาคาร หรือความเสียหายต่อระบบเศรษฐกิจ และเสถียรภาพทางการเงินการธนาคารของประเทศได้อย่างมหาศาล

แต่ในทางกลับกัน ประเทศไทยกลับมีบทบัญญัติที่บังคับใช้กับการกระทำอาชญากรรมโดยทั่วๆ ไปเท่านั้นเช่น ความผิดฐานลักทรัพย์ วิ่งราวทรัพย์ ชิงทรัพย์ ปล้นทรัพย์ ซึ่งเห็นได้ชัดว่า

กฎหมายอาญาไทยมุ่งเน้นเฉพาะอาชญากรรมที่มีรูปแบบที่รุนแรงที่สามารถเห็นได้ชัด หรืออาจส่งผลกระทบต่อชีวิต และทรัพย์สินของประชาชน แต่อาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ เช่น อาชญากรรมต่อกระบวนการโอนเงินทางอิเล็กทรอนิกส์ หรืออาชญากรรมที่ใช้กระบวนการโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิดนั้น ล้วนแล้วแต่สามารถสร้างความเสียหายต่อระบบเศรษฐกิจหรือระบบการเงินการธนาคารได้อย่างมหาศาล แต่ปัจจุบันประเทศไทยกลับไม่มีกฎหมายในการบังคับใช้กับอาชญากรรมลักษณะนี้ไว้โดยตรง ด้วยช่องว่างทางกฎหมาย หรือการไม่มีมาตรการทางกฎหมายที่ชัดเจนในการบังคับใช้กับอาชญากรรมดังกล่าวอาจส่งผลทำให้มีอาชญากรรมประเภทนี้มากยิ่งขึ้น ผู้กระทำความผิดขาดการเกรงกลัวต่อบทบัญญัติแห่งกฎหมาย หรืออาจส่งให้มีลักษณะการกระทำที่สร้างความเสียหายได้มากยิ่งขึ้นเรื่อยๆ อันเป็นผลทำให้ประชาชน หรือระบบธุรกิจการเงินการธนาคารภายในประเทศและระหว่างประเทศอาจขาดความน่าเชื่อถือ หรือขาดความไว้วางใจในภาคการเงินการธนาคารของประเทศไทย อันเป็นผลกระทบอย่างมากต่อเสถียรภาพ และความมั่นคงของระบบการเงินการธนาคารของประเทศชาติและระบบเศรษฐกิจของประเทศ ซึ่งหากพิจารณาถึงสาเหตุดังกล่าวจะเห็นได้ว่าช่องว่างของกฎหมายดังกล่าว เป็นปัญหาและอุปสรรคต่อการบังคับใช้กฎหมายของประเทศไทยเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์อย่างยิ่ง ดังนั้นประเทศไทยจึงควรมีศึกษาถึงมาตรการทางกฎหมายที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ว่า ควรมีแนวทางแก้ไขอย่างไร โดยศึกษาเปรียบเทียบกับมาตรการทางกฎหมายต่างประเทศที่บังคับใช้กับการกระทำอาชญากรรมดังกล่าวว่ามีมาตรการหรือแนวทางบังคับใช้กฎหมาย เพื่อเป็นแนวทางในการปรับปรุงกฎหมายของประเทศไทยต่อไป

1.2. วัตถุประสงค์ของการศึกษาวิจัย

1. เพื่อศึกษาวิเคราะห์ถึงปัญหาและการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์
2. เพื่อศึกษาถึงปัญหาหรืออุปสรรคของการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในประเทศไทย
3. เพื่อศึกษาถึงปัญหาหรืออุปสรรคของหน่วยงานที่มีหน้าที่บังคับใช้กฎหมายกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ลักษณะนี้
4. เพื่อศึกษา วิเคราะห์มาตรการทางกฎหมายที่เหมาะสมในการบังคับใช้กับการกระทำความผิดต่อระบบโอนเงินทางอิเล็กทรอนิกส์ในประเทศไทย เพื่อแก้ไขเพิ่มเติม หรือปรับปรุงกฎหมายไทยในการกำหนดบทบัญญัติแห่งกฎหมายให้มีความทันสมัย และสามารถบังคับใช้กับอาชญากรรมที่เกิดขึ้นในระบบโอนเงินทางอิเล็กทรอนิกส์ เพื่อให้

หน่วยงานที่มีหน้าที่บังคับใช้กฎหมายกับอาชญากรรมลักษณะนี้ สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ เพื่อเป็นการคุ้มครองการโอนเงินทางอิเล็กทรอนิกส์ภายใต้ระบบการเงินการธนาคารให้มีความน่าเชื่อถือ หรือมีความปลอดภัยเพียงพอต่อระบบการเงินการธนาคารของประเทศ

1.3. สมมติฐานของการศึกษาวิจัย

ความล้ำหน้าทางเทคโนโลยีของกระบวนการโอนเงินทางอิเล็กทรอนิกส์ของระบบการเงินการธนาคารในปัจจุบัน ได้เข้ามาพัฒนาการทางด้านการให้บริการการโอนเงินทางอิเล็กทรอนิกส์ แต่กระบวนการดังกล่าวกลับถูกใช้เป็นเครื่องมือจากผู้ทุจริตในการแสวงหาผลประโยชน์ ซึ่งหากพิจารณาถึงกฎหมายไทยแล้ว มีการบัญญัติกฎหมายที่บังคับใช้กับอาชญากรรมดังกล่าวที่ไม่เพียงพอกับสภาพปัญหาที่เกิดขึ้นในปัจจุบัน ด้วยเหตุนี้จึงเป็นปัญหาและอุปสรรคอย่างยิ่งต่อการบังคับใช้กฎหมาย ซึ่งผู้ศึกษาเห็นว่าควรมีการศึกษาถึงมาตรการทางกฎหมายต่างประเทศที่บังคับใช้กับกรณีดังกล่าว เพื่อนำมาเป็นแนวทางในการปรับปรุงกฎหมายไทยให้มีมาตรการทางกฎหมายในลักษณะต่างๆเพื่อให้สามารถบังคับใช้กับอาชญากรรมดังกล่าวได้อย่างมีประสิทธิภาพ

1.4. วิธีดำเนินการวิจัย

การดำเนินการวิจัยในลักษณะเชิงเอกสาร (Documentary Research) ซึ่งมีการศึกษารวบรวมข้อมูลจากแหล่งตำราต่างๆ เช่น ตำรา บทความ หรือกฎหมาย หรือการศึกษาข้อมูลจากมาตรการของต่างประเทศ ที่เกี่ยวข้องกับมาตรการทางกฎหมายที่บังคับใช้กับอาชญากรรมทางคอมพิวเตอร์ที่เกิดขึ้นในกระบวนการโอนเงินอิเล็กทรอนิกส์ เพื่อทำการเปรียบเทียบกับมาตรการของประเทศไทยที่มีอยู่ในปัจจุบัน

1.5. ขอบเขตของการศึกษาวิจัย

การศึกษาวิจัยเรื่องนี้มุ่งศึกษาถึงมาตรการทางกฎหมายที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในประเทศไทย โดยศึกษาเปรียบเทียบกับมาตรการทางกฎหมายในต่างประเทศที่วางมาตรการทางกฎหมายในลักษณะต่างๆ ในการบังคับใช้กับอาชญากรรมที่เกิดขึ้นกับกระบวนการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าว

1.6. ประโยชน์ที่คาดว่าจะได้รับจากการศึกษาวิจัย

1. ทำให้ทราบถึงปัญหาและอุปสรรคของการบังคับใช้กฎหมายของไทยกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในประเทศไทย
2. ทำให้ทราบถึงมาตรการทางกฎหมายต่างประเทศที่ใช้บังคับกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินอิเล็กทรอนิกส์ เพื่อหามาตรการหรือแนวทางที่เหมาะสมในการแก้ไขเพิ่มเติมหรือปรับปรุงกฎหมายของประเทศไทยต่อไป อันจะส่งผลให้การบังคับใช้กฎหมายกับอาชญากรรมดังกล่าวเป็นไปได้อย่างมีประสิทธิภาพ
3. ศึกษาถึงแนวทางการดำเนินงานที่เหมาะสมขององค์กร หน่วยงานที่มีหน้าที่ดูแลควบคุม ดูแลระบบการโอนเงินทางอิเล็กทรอนิกส์ หรือมีอำนาจหน้าที่ในการบังคับใช้กฎหมายกับอาชญากรรมต่างๆ ที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ เพื่อรองรับกับการบังคับใช้กฎหมายอาญาให้เป็นไปได้อย่างมีประสิทธิภาพ
4. สามารถนำข้อคิดเห็น บทสรุป ข้อเสนอแนะจากการศึกษาครั้งนี้ไปใช้ในการวางมาตรการหรือแนวทางที่เหมาะสมในการแก้ไขเพิ่มเติม ปรับปรุงกฎหมายไทยให้ทันสมัยทัดเทียมเทคโนโลยีของอาชญากรรมที่เกิดขึ้นได้อย่างเป็นรูปธรรม

บทที่ 2

เงินและการโอนเงินทางอิเล็กทรอนิกส์กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

2.1 ความรู้ทั่วไปเกี่ยวกับเงิน

นับตั้งแต่อดีตจนถึงปัจจุบันมนุษย์มีวิถีชีวิตที่เกี่ยวข้องกับเงินเรื่อยมา โดยการดำรงชีวิตของมนุษย์นั้นจำเป็นต้องมีหรือใช้สินค้าและบริการต่างๆ อันเป็นปัจจัยพื้นฐานสำหรับการดำรงชีพของมนุษย์ เงินจึงกลายเป็นสื่อกลางของการชำระราคาสินค้าหรือบริการต่างๆ รวมทั้งเป็นสื่อกลางในการดำเนินธุรกิจการค้า ธุรกิจการพาณิชย์ต่างๆ และการแลกเปลี่ยนสินค้าและบริการต่างๆ ระหว่างกัน เงินจึงจัดได้ว่าเป็นสิ่งจำเป็นอย่างยิ่งในการดำรงชีวิตของมนุษย์ในสังคมและเป็นองค์ประกอบสำคัญของสังคม ประกอบกับปัจจุบันในแต่ละสังคมได้มีการพัฒนารูปแบบของเงินให้มีความหลากหลาย สะดวกสบาย และคล่องตัวต่อการใช้ประโยชน์เพิ่มมากยิ่งขึ้น โดยปัจจุบันแต่ละประเทศได้มีการตราเงินตราสกุลต่างๆ ของตนเอง ไม่ว่าจะเป็น เงินบาท เงินยูโร เงินดอลลาร์ เงินเยน เพื่อใช้ภายในประเทศ

2.1.1 ความหมายของเงิน

ตามพจนานุกรมฉบับราชบัณฑิตยสถานได้ให้คำนิยามคำว่า "เงิน" หมายถึง แร่สีขาวเนื้ออ่อน ; วัตถุที่ชำระหนี้ได้ตามกฎหมาย, วัตถุที่ใช้วัดราคาในการซื้อขายแลกเปลี่ยนกัน, โบราณใช้คำว่า งึน, เง็น หรือเงือนก็มี หรือคำนิยามคำว่า"เงิน" ในแง่ของกฎหมายนั้น "เงิน" หมายถึง สิ่งที่ชำระหนี้ได้ตามกฎหมาย แต่ในแง่ของหลักเศรษฐศาสตร์คำนิยามของคำว่า "เงิน" หมายถึง สิ่งที่ทุกคนในสังคมยอมรับเป็นสื่อกลางในการแลกเปลี่ยน (medium of exchange) และวัดมูลค่าของสินค้าและบริการทุกชนิด (standard of value)[1] ซึ่งเงินที่เรียกกันโดยทั่วไปไม่ว่าจะเป็นเงินสดหรือเงินตรา ตามพจนานุกรมฉบับราชบัณฑิตยสถานได้ให้ความหมายไว้แตกต่างกัน กล่าวคือ "เงินตรา" หมายถึง วัตถุที่มีตราของรัฐบาลใช้ชำระหนี้ได้ตามกฎหมาย และ "เงินสด" หมายถึง เงินที่มีอยู่กับตนหรืออาจจ่ายได้ทันที, เงินที่ชำระให้ทันทีเมื่อซื้อหรือขายกัน

---

[1] สุรักษ์ บุนนาค และวณี ฉ่อยเกียรติกุล, การเงินและการธนาคาร (กรุงเทพฯ: สำนักพิมพ์ไทยวัฒนาพาณิช จำกัด, 2541), หน้า 1.

อย่างไรก็ตามไม่ว่าจะกล่าวถึง "เงิน" ในลักษณะใด "เงิน" หมายถึง วัตถุใดๆ หรือสิ่งหนึ่งสิ่งใดที่มูลค่าชี้วัดอันเป็นมาตรฐานซึ่งทุกคนให้การยอมรับ เพื่อให้เป็นสื่อกลางในการแลกเปลี่ยนหรือชำระราคาสินค้าและบริการต่างๆ รวมทั้งสามารถอ้างอิงมูลค่าชี้วัดและสามารถนำมาชำระหนี้ได้ตามกฎหมาย

2.1.2 วิวัฒนาการของเงิน

แต่เดิมเงินที่ใช้เป็นสื่อกลางในการดำเนินธุรกิจค้าขาย ธุรกิจการพาณิชย์ต่าง ๆ นั้น ได้ใช้สินค้าที่โดยทั่วไปให้การยอมรับ และเป็นสินค้าที่มีมีการวางมาตรฐานมูลค่าในตัวสินค้านั้นไว้ เพื่อให้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าหรือบริการต่าง ๆ ที่ต้องการ โดยส่วนใหญ่สินค้าที่นำมาใช้แทนเงินดังกล่าวมักเป็นสินค้าที่มีความสำคัญทางเศรษฐกิจ ได้รับความนิยมและมีมูลค่าในตัวเองจึงสามารถนำมาใช้แทนการชำระราคาของสินค้าหรือบริการที่ต้องการได้ ซึ่งสินค้าที่มีมูลค่าแทนเงินดังกล่าว ได้แก่ ขนสัตว์ หนังสัตว์ ใบชา ยาสูบ เกลือ แพะ พรม อัญมณี เป็นต้น

ต่อมาธุรกิจการค้าขาย ธุรกิจการพาณิชย์ต่าง ๆ ได้มีการขยายตัวมากขึ้น การนำสินค้าใช้ชำระราคาแทนเงินจึงประสบปัญหา เนื่องจากสินค้าที่ใช้แทนเงินนั้นขาดความแน่นอนในมูลค่าราคา ไม่อาจแบ่งมูลค่าแยกย่อยได้ ไม่สะดวกต่อการเคลื่อนย้ายหรือการโอนเงินดังกล่าว และขาดความคงทนถาวร ดังนั้นเงินจึงได้มีการพัฒนาออกมาในลักษณะต่างๆ ต่อไปนี้

2.1.2.1 โลหะหรือเงินโลหะ

ในอดีตการนำโลหะที่มีค่ามาใช้แทนเงินในแบบเดิมนั้น จะเป็นการนำน้ำหนักของโลหะที่มีค่านั้นมาเปรียบเทียบเป็นมูลค่า และแลกเปลี่ยนหรือใช้ชำระราคาสินค้าหรือบริการต่าง ๆ ที่ต้องการ ให้เป็นไปตามมูลค่าราคาของโลหะเทียบกับมูลค่าราคาของสินค้าหรือบริการต่างๆ ดังกล่าว ซึ่งโลหะที่นิยมนำมาใช้เป็นเงินได้แก่ เงินและทองคำ หลังจากนั้นได้มีการพัฒนาในการนำโลหะที่มีค่าดังกล่าวมาหลอมเป็นเงินเหรียญทำให้มูลค่าของเงินมีเกณฑ์ในการชี้วัดราคาที่มีความแน่นอนมากขึ้น เก็บรักษาได้ยาวนานและสามารถเคลื่อนย้ายถ่ายโอนได้สะดวกมากขึ้น อย่างไรก็ตามเงินโลหะหรือเงินเหรียญนั้นมีน้ำหนักมาก และไม่สะดวกต่อการพกพาการเคลื่อนย้ายหรือการโอนเท่าที่ควร ดังนั้นพ่อค้าหรือนักธุรกิจจึงได้พัฒนาการชำระราคาด้วยเงินโลหะให้มีการรับฝากเงินโลหะแทนการพกพา การโอนหรือการเคลื่อนย้ายเงินเพื่อชำระราคาระหว่างกัน โดยการชำระราคาสินค้าหรือบริการต่างๆ ให้ใช้ใบรับฝากเงินที่ระบุมูลค่าตามเงินโลหะที่ฝากไว้นั้นเป็นตราสารในการชำระเงิน ซึ่งในสมัยนั้นผู้ทำหน้าที่รับฝากเงินส่วนใหญ่จะเป็น

นายช่างทอง และหากเปรียบเทียบกับปัจจุบันก็มีลักษณะเดียวกับธนาคารพาณิชย์ที่ทำหน้าที่รับฝากเงิน และออกใบรับฝากเงินเป็นหลักฐานให้แก่ลูกค้า ซึ่งระบบธนาคารจึงได้พัฒนาใบรับฝากเงินดังกล่าวมาเป็นการออกบัตรเงินฝาก เพื่อเป็นหลักฐานในการทำธุรกรรมทางการเงินต่าง ๆ ของลูกค้า ซึ่งความหมายของคำว่า "บัตรเงินฝาก" ตามนัยแห่งพระราชบัญญัติธนาคารพาณิชย์ พ.ศ. 2505 (แก้ไขเพิ่มเติมฉบับที่ 3) พ.ศ. 2535 มาตรา 4 [2] ได้คำนิยามคำว่า "บัตรเงินฝาก" หมายถึง ตราสารซึ่งเปลี่ยนมือได้ที่ธนาคารพาณิชย์ออกให้แก่ผู้ฝากเงินเพื่อเป็นหลักฐานการรับฝากเงิน และเพื่อแสดงสิทธิของผู้ทรงตราสารที่จะได้รับเงินฝากคืนเมื่อสิ้นระยะเวลาอันกำหนดไว้ โดยจะมีการกำหนดดอกเบี้ยไว้ด้วยหรือไม่ก็ได้

2.1.2.2 เงินกระดาษหรือตราสารประเภทต่างๆ

วิวัฒนาการลำดับต่อมาของเงินคือ การใช้เงินกระดาษในการชำระเงินมูลค่าสินค้าหรือบริการต่างๆ เพื่อความสะดวกในการให้บริการ จนกระทั่งในปัจจุบันเงินได้มีการพัฒนารูปแบบให้มีมูลค่าชี้วัดที่แน่นอน สะดวกต่อการพกพาเคลื่อนย้ายหรือการโอนโดยการนำกระดาษมาใช้แทนเงิน หรือที่เรียกทั่วไปในปัจจุบันว่า "ธนบัตร" ซึ่งพจนานุกรมฉบับราชบัณฑิตยสถานได้ให้ความนิยามคำว่า "ธนบัตร" หมายถึง บัตรที่ใช้แทนเงินตรา ดังนั้นในการชำระเงินโดยใช้ธนบัตรจึงทำให้ธนบัตรเป็นเงินพื้นฐานที่ได้รับความนิยม และได้รับการยอมรับมากที่สุดรองจากเงินโลหะ ซึ่งในปัจจุบันได้มีการนำธนบัตรและเหรียญโลหะต่างๆ กำหนดให้เป็นเงินตราสกุลต่างๆ มากมาย เช่น เงินดอลลาร์ เงินบาท เงินปอนด์เงินเยน เป็นต้น เช่นเดียวกับระบบการชำระเงินของประเทศไทยปัจจุบันที่ได้มีการพัฒนาหน่วยเงินตราของไทยเป็นลำดับ ซึ่งปัจจุบันประเทศไทยได้กำหนดให้เงินบาทเป็นหน่วยเงินตราพื้นฐานในการทำหน้าที่เป็นสื่อกลางทางการพาณิชย์ เพื่อการชำระราคาสินค้าและบริการต่างๆ ระหว่างกัน

2.1.2.3 เงินอิเล็กทรอนิกส์

ในปัจจุบันธนาคารพาณิชย์ หรือผู้ประกอบธุรกิจทางด้านธนาคารพาณิชย์ได้เสนอบริการทางการเงินในรูปแบบใหม่ในรูปแบบของอิเล็กทรอนิกส์ หรือที่เรียกโดยทั่วไปว่าเงินอิเล็กทรอนิกส์ (E-money) เพื่ออำนวยความสะดวกในการชำระเงินในลักษณะต่างๆ ซึ่งเงินอิเล็กทรอนิกส์ได้มีการพัฒนาในการให้บริการในรูปแบบต่างๆ ต่อไปนี้

---

[2] พระราชบัญญัติธนาคารพาณิชย์ พ.ศ. 2505 (แก้ไขเพิ่มเติมฉบับที่ 3) พ.ศ.2535., แหล่งที่มา : http://203.152.23.33/law/text/lawpub/lawa021/text.html.

1. บัตรพลาสติกที่บรรจุไมโครชิพ (Smart Card) ซึ่งผู้ถือบัตรสามารถขอให้ผู้ออกบัตรบรรจุเงินอิเล็กทรอนิกส์ (E-money) ไว้ลงในบัตรและบัตรดังกล่าวจะใช้เงินอิเล็กทรอนิกส์นั้นในการชำระค่าสินค้าและบริการแก่ผู้ขายสินค้าผ่านเครื่อง EDC (Electronic Data Capture) โดยเครื่อง EDC ดังกล่าวจะทำการตรวจสอบยอดเงินอิเล็กทรอนิกส์ (E-money) ที่บรรจุอยู่และหักเงินอิเล็กทรอนิกส์นั้น เพื่อชำระค่าสินค้าและบริการดังกล่าวจากเงินอิเล็กทรอนิกส์ ที่บรรจุไว้ในบัตรพลาสติกดังกล่าว นอกจากนั้นในกรณีที่เงินอิเล็กทรอนิกส์ที่บรรจุอยู่ในบัตรหมดลงผู้ถือบัตรดังกล่าวสามารถขอเติมเงินอิเล็กทรอนิกส์จากผู้ออกบัตรได้ ซึ่งบัตรที่มีลักษณะดังกล่าวนี้ได้มีการให้บริการอยู่ในต่างประเทศ ได้แก่ Mondex Card และ Visa Card ซึ่งใช้อยู่ในต่างประเทศและมีแนวโน้มว่าจะมีการนำเข้ามาให้บริการในประเทศไทยด้วย
2. การใช้เงินอิเล็กทรอนิกส์ผ่านเครือข่ายอินเทอร์เน็ต ไม่ว่าจะเป็นในรูปของเช็คอิเล็กทรอนิกส์หรือบัตรเครดิต ซึ่งเงินอิเล็กทรอนิกส์ (E-money) ในรูปของเช็คอิเล็กทรอนิกส์ (Electronic cheque) เป็นการใช้เงินอิเล็กทรอนิกส์ที่ผู้ใช้บริการสามารถขอดาวน์โหลด (download) เงินอิเล็กทรอนิกส์จากธนาคารหรือผู้ที่ออกเงินอิเล็กทรอนิกส์ลงในเครื่องคอมพิวเตอร์ของตน และใช้เงินอิเล็กทรอนิกส์นั้นในการโอนเงินอิเล็กทรอนิกส์จากเครื่องคอมพิวเตอร์ของตนให้แก่ผู้ขายสินค้า เพื่อชำระราคาค่าสินค้าและบริการนั้น หรือโอนเงินอิเล็กทรอนิกส์จากบัตรเครดิตของตนเพื่อชำระราคาค่าสินค้าและบริการต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ท ซึ่งระบบดังกล่าวสามารถช่วยในการอำนวยความสะดวกทางการเงินการธนาคาร และมีความเป็นไปได้ที่จะมีผู้ใช้บริการเงินอิเล็กทรอนิกส์ (E-money) นี้เพิ่มมากขึ้นในอนาคต

นอกจากนี้ หากกล่าวถึง เงิน ในมุมมองของมูลค่าแห่งเงินอาจแบ่งได้ออกเป็น 2 ลักษณะ กล่าวคือ มูลค่าภายนอกและมูลค่าภายใน ซึ่งมูลค่าภายนอกของเงินคือราคาแห่งเงินตราสกุลหนึ่งๆ เมื่อคิดเป็นราคาของเงินตราอีกสกุลหนึ่ง หรือกล่าวอีกนัยหนึ่งว่า อัตราแลกเปลี่ยนเงินตราต่างประเทศ และมูลค่าภายในของเงินคือ อำนาจซื้อสินค้าและบริการของเงินในแต่ละสกุลในประเทศนั้น ซึ่งมูลค่าของเงินดังกล่าวเป็นมูลค่าที่มีราคา มีอัตราชี้วัดได้แน่นอน และได้รับการยอมรับโดยทั่วไป โดยมูลค่าแห่งเงินดังกล่าวนั้นเรียกกันโดยทั่วไปว่า"ค่าเงิน" ซึ่งค่าของเงินดังกล่าวนั้นอาจเปลี่ยนแปลงได้ตามสภาพเศรษฐกิจของประเทศและเศรษฐกิจทั่วโลก แล้วแต่ว่า

นโยบายของรัฐบาลในประเทศนั้นกำหนดให้เงินตราของประเทศมีมูลค่าผันผวนได้ตามสภาพเศรษฐกิจหรือไม่ หรือที่เรียกว่า "อัตราลอยตัว" หรือรัฐบาลแห่งประเทศนั้นกำหนดให้ค่าเงินในประเทศมีอัตรามาตรฐานแล้วแต่กรณี ยกตัวอย่างเช่น เดิมค่าเงินบาทในประเทศไทยมีอัตราแลกเปลี่ยนเงินตราระหว่างประเทศที่แน่นอน แต่ปัจจุบันค่าเงินบาทใช้อัตราลอยตัว ดังนั้นค่าเงินบาทในประเทศไทยจึงมีอัตราที่เปลี่ยนแปลงไปตามสภาพเศรษฐกิจและสถานการณ์โลก

2.2 ระบบการเงินการธนาคารในประเทศไทย

2.2.1 วิวัฒนาการของระบบธนาคารพาณิชย์ในประเทศไทย

ธนาคารพาณิชย์ในประเทศไทยได้เริ่มจัดตั้งขึ้นตั้งแต่ในสมัยพระบาทสมเด็จพระจุลจอมเกล้าเจ้าอยู่หัวที่มีพระราชประสงค์ให้การค้าขายระหว่างประเทศในประเทศไทย มีความเจริญก้าวหน้าดังในต่างประเทศจึงมีประราชประสงค์ในการปรับปรุงระบบการธนาคารในประเทศไทย โดยในขณะนั้นประเทศไทยมีธนาคารพาณิชย์ของอังกฤษ 2 ธนาคาร ได้แก่ ธนาคารฮ่องกงและเซี่ยงไฮ้ (Hong Kong & Shanghai Banking Corp.) เป็นธนาคารแรกที่ได้พระบรมราชานุญาตให้จัดตั้งขึ้นเมื่อพ.ศ.2431และธนาคารชาร์เตอร์ (The Charter Bank Ltd.) ซึ่งตั้งขึ้นในปี พ.ศ. 2437 เป็นธนาคารแห่งที่สอง และธนาคารแห่งอินโดจีน (Banque de L'Indochine Ltd.) ซึ่งเป็นของฝรั่งเศสและจัดตั้งขึ้นในปี พ.ศ.2440 เป็นธนาคารแห่งที่สาม ซึ่งธนาคารต่างชาติที่จัดตั้งขึ้นในสมัยนั้นมักมุ่งเน้นการค้าขายระหว่างประเทศที่เอื้อประโยชน์ให้แก่การค้าขายของบุคคลในชาติของตนเป็นหลัก โดยไม่ได้อำนวยประโยชน์ให้แก่พ่อค้าคนไทยเท่าใดนัก

ต่อมาระบบการเงินการธนาคารเป็นที่นิยมในประเทศไทยมากขึ้น พระบาทสมเด็จพระจุลจอมเกล้าเจ้าอยู่หัวจึงทรงโปรดเกล้าให้เปิดกิจการที่ดำเนินการเช่นเดียวกับธนาคารพาณิชย์ในสมัยนั้น เป็นกิจการทดลองเป็นการภายในตั้งแต่เดือนตุลาคม พ.ศ. 2447 เพื่อรับฝากเงินจากกลุ่มคนที่มีความเชื่อถือและให้กู้ยืม โดยพระราชทานนามกิจการว่า "บุคคลัภย์ (Book Club) " ต่อมากิจการดังกล่าวเริ่มได้รับความนิยม และได้รับความเชื่อถือมากขึ้นจึงได้ขอพระราชทานพระบรมราชานุญาตให้จัดตั้งเป็นธนาคารชื่อ "แบงค์สยามกัมมาจล ทุนจำกัด (Siam Commercial Bank Co., Ltd.)" เมื่อวันที่ 1 เมษายน พ.ศ. 2449 โดยให้ดำเนินธุรกิจธนาคารพาณิชย์เช่นเดียวกับธนาคารพาณิชย์ของชาติตะวันตก และให้ขยายกิจการเพื่อธุรกิจด้านแลกเปลี่ยนเงินตราต่างประเทศด้วย จนกระทั่งในวันที่ 27 มกราคม พ.ศ. 2482 ได้มีการเปลี่ยนชื่อแบงค์สยามกัมมาจล ทุนจำกัดเป็นธนาคารไทยพาณิชย์ จำกัด ซึ่งถือเป็นธนาคารพาณิชย์แห่งแรกในประเทศไทย

ต่อมาจนถึงปัจจุบัน ประเทศไทยได้มีการพัฒนาและจัดตั้งธนาคารพาณิชย์เพิ่มมากขึ้นตามลำดับ และได้มีการจัดตั้งสถาบันทางการเงินอื่นๆ ที่สามารถให้บริการทางการเงินได้เช่นเดียวกับธนาคารพาณิชย์ ซึ่งหากพิจารณาจากความหมายของ "การธนาคารพาณิชย์" และ "ธนาคารพาณิชย์" แล้วตามพระราชบัญญัติธนาคารพาณิชย์ พ.ศ. 2505 (แก้ไขเพิ่มเติมฉบับที่ 2) พ.ศ.2522 ได้ให้คำจำกัดความของ "การธนาคารพาณิชย์" และ "ธนาคารพาณิชย์" [3] ไว้ในมาตรา 4 กล่าวคือ

"การธนาคารพาณิชย์" หมายความว่า การประกอบธุรกิจประเภทรับฝากเงินที่ต้องจ่ายคืนเมื่อทวงถาม หรือเมื่อสิ้นระยะเวลาอันกำหนดไว้และใช้ประโยชน์เงินนั้นในทางหนึ่งหรือหลายทาง เช่น (ก) ให้สินเชื่อ (ข) ซื้อขายตั๋วแลกเงิน หรือตราสารเปลี่ยนมืออื่นใด (ค) ซื้อขายเงินปริวรรตต่างประเทศ

"ธนาคารพาณิชย์" หมายความว่า ธนาคารที่ได้รับอนุญาตให้ประกอบการธนาคารพาณิชย์ และหมายความรวมถึงสาขาของธนาคารต่างประเทศที่รับอนุญาตให้ประกอบการธนาคารพาณิชย์ด้วย

จากตามคำนิยามข้างต้นจึงสรุปได้ว่า ธนาคารพาณิชย์ในประเทศไทยหรือธนาคารสาขาของธนาคารต่างประเทศที่ดำเนินกิจการธนาคารพาณิชย์ในประเทศไทย ต้องได้รับการอนุญาตให้ประกอบกิจการการธนาคารพาณิชย์ โดยการอนุญาตดังกล่าว ธนาคารพาณิชย์หรือสถาบันการเงินที่ให้บริการการธนาคารพาณิชย์ต้องอยู่ภายใต้การกำกับ ดูแล และการควบคุมการดำเนินงานการธนาคารพาณิชย์ของธนาคารแห่งประเทศไทย ตามระบบการเงินการธนาคารสากลที่จะต้องมีการจัดตั้งธนาคารกลางขึ้นในการทำหน้าที่กำกับดูแล ควบคุม และวางมาตรการต่างๆ ในการควบคุมระบบการชำระเงินภายในประเทศนั้นๆ ให้เป็นไปตามนโยบาย กฎ และระเบียบต่างๆ ที่ธนาคารกลางเป็นผู้กำหนด เพื่อให้การจัดระบบการชำระเงินภายในประเทศสามารถดำเนินไปได้อย่างดี และมีประสิทธิภาพอันสามารถอำนวยประโยชน์สูงสุดให้แก่ระบบการเงินการธนาคารของประเทศนั้น ๆ และสามารถสร้างเสถียรภาพทางการเงินและความมั่นคงทางการเงินให้แก่ประเทศได้ ซึ่งธนาคารกลางที่ได้ถูกจัดตั้งขึ้นและมีบทบาทหน้าที่ในการกำกับดูแล ควบคุมธุรกรรมทางการเงินต่างๆ ภายในประเทศได้แก่ ธนาคารแห่งประเทศไทย ซึ่งถูกจัดตั้งขึ้นตามพระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485 โดยสามารถสรุปบทบาทของธนาคารแห่งประเทศไทยต่อระบบการเงินการธนาคารของไทยได้ดังต่อไปนี้

---

[3] พระราชบัญญัติธนาคารพาณิชย์ พ.ศ. 2505 (แก้ไขเพิ่มเติมฉบับที่ 2) พ.ศ. 2522, แหล่งที่มา : http://203.152.23.33/law/text/lawpub/lawa021/text.html.

1. การออกและพิมพ์ธนบัตร หรือตราเหรียญกษาปณ์ของเงินบาทไทย
2. การควบคุม กำกับดูแลการให้บริการของธนาคารพาณิชย์ในประเทศไทย เช่น การรักษาบัญชีเงินฝากของธนาคารพาณิชย์, การเป็นสำนักงานกลางในการหักบัญชีอิเล็กทรอนิกส์, การให้กู้ยืมเงินแหล่งสุดท้าย และการเป็นศูนย์กลางการโอนเงินทางอิเล็กทรอนิกส์ เป็นต้น
3. การควบคุมระบบการชำระเงินของรัฐบาลเช่นการรักษาบัญชีเงินฝากของหน่วยงานรัฐบาลและรัฐวิสาหกิจ, การซื้อขายเงินตราต่างประเทศให้หน่วยราชการ, การให้เงินกู้เพื่อชดเชยการขาดดุลในเงินงบประมาณ, การให้เงินกู้เพื่อใช้จ่ายตามโครงการเฉพาะอย่างของรัฐบาลหรือรัฐวิสาหกิจ
4. การดำเนินกิจการระหว่างประเทศ เช่นการจัดหนี้สาธารณะ, การกำหนดอัตราเงินสดสำรองตามกฎหมาย, การกำหนดอัตราดอกเบี้ยเงินให้กู้ยืมและอัตราการรับช่วงซื้อลดตั๋วสัญญาใช้เงิน, การกำหนดอัตราส่วนเงินกองทุนต่อสินทรัพย์ภายในประเทศ,การกำหนดอัตราส่วนให้กู้ยืมแก่บุคคลใดบุคคลหนึ่งต่อเงินกองทุน หรือการกำหนดการให้สินเชื่อแก่กิจการประเภทหนึ่งประเภทใด, การกำหนดอัตราดอกเบี้ยเงินฝากและเงินให้กู้ยืมของธนาคารพาณิชย์
5. การควบคุมธุรกรรมการแลกเปลี่ยนเงินของประเทศหรือการโอนเงินระหว่างประเทศ
6. การวางมาตรการควบคุมการขยายตัวและการดำเนินงานของธนาคารพาณิชย์ให้อยู่ภายใต้ขอบเขตของกฎหมายและระเบียบแห่งธนาคารแห่งประเทศไทยได้ประกาศไว้ และช่วยเหลือและส่งเสริมธนาคารพาณิชย์ในทุกๆ ทางที่เห็นสมควร

ธนาคารแห่งประเทศไทยจึงมีบทบาทสำคัญต่อระบบการเงินและการธนาคารในการกำกับ ดูแล ควบคุมระบบการชำระเงินของประเทศไทยให้สามารถดำเนินไปได้อย่างมีเสถียรภาพ และสนับสนุน และส่งเสริมการธนาคารพาณิชย์ภายใต้ระบบการชำระเงินของประเทศไทยให้สามารถดำเนินไปได้อย่างสะดวกและรวดเร็วและมีประสิทธิภาพสูงสุด ส่วนธนาคารพาณิชย์ไทยได้มีบทบาทสำคัญต่อระบบการเงินการธนาคารของประเทศ ในการเป็นผู้ให้บริการทางการเงินในรูปแบบต่างๆ ผ่านระบบการชำระเงินภายในประเทศและระบบการชำระเงินระหว่างประเทศ

2.2.2 วิวัฒนาการของระบบการชำระเงินในประเทศไทย

เนื่องด้วยในอดีตการชำระเงินค่าราคาสินค้า หรือบริการต่าง ๆ ในการซื้อขายสินค้าหรือการกระทำการค้าขายเชิงพาณิชย์นั้นจะใช้วิธีการแลกเปลี่ยนสินค้าระหว่างผู้ซื้อกับผู้ขายโดยตรง โดยเป็นการนำสินค้าที่มีมูลค่าใกล้เคียงกันมาแลกเปลี่ยนซึ่งกันและกัน และในระยะเวลาต่อมาเมื่อมีการกำหนดให้เงินหรือที่เรียกกันโดยทั่วไปว่า เงินสด (cash) มาเป็นสื่อกลางทางการค้าหรือการพาณิชย์เพื่อชำระราคาสินค้าและบริการต่างๆ ระหว่างกัน ประกอบกับการซื้อขายสินค้าหรือการค้าขายได้มีการขยายตัวมากขึ้น ระบบการชำระเงินจึงได้มีการพัฒนาในการกำหนดสื่อกลางในการชำระเงินจากการแลกเปลี่ยนหรือการส่งมอบสินค้าต่างๆ แทนการชำระเงินเป็นการแลกเปลี่ยนหรือการส่งมอบเงิน ไม่ว่าจะเป็นเงินในรูปแบบของเงินโลหะ เงินธนบัตร หรือเงินในลักษณะอื่นๆ หลังจากนั้นระบบการชำระเงินจึงได้มีการพัฒนากระบวนการในการชำระเงินให้มีความรวดเร็ว และสะดวกมากขึ้นตามสภาพเศรษฐกิจ สภาพสังคม เทคโนโลยีทางคอมพิวเตอร์ที่ได้มีการพัฒนา และนำความเจริญก้าวหน้าของระบบคอมพิวเตอร์และเทคโนโลยีสารสนเทศมาใช้ในการพัฒนาระบบชำระเงินให้สามารถดำเนินไปได้อย่างทันสมัย สะดวกและรวดเร็ว

ระบบคอมพิวเตอร์และเทคโนโลยีสารสนเทศจึงได้เข้ามามีบทบาทและมีความสำคัญต่อธุรกิจการค้า ธุรกิจการธนาคารพาณิชย์ และระบบการชำระเงินเพิ่มมากขึ้นตามลำดับ ระบบการชำระเงินจึงได้พัฒนารูปแบบหรือสื่อกลางการชำระเงินจากเดิมที่เป็นระบบการชำระเงินด้วยเงินสดเปลี่ยนเป็นการใช้ระบบการชำระเงินประเภทอื่น ๆ แทนเงินสด ไม่ว่าจะเป็น การชำระเงินโดยใช้ตราสารต่างๆ ไม่ว่าจะเป็น ดร๊าฟท์ (Draft) , เช็ค (Cheque), เช็คเดินทาง (Traveller's Cheque) , ตราสารที่ระบุคำสั่งทางการเงิน (Money Order), ธนาณัติ (Postal Order) หรือตราสารชนิดหนึ่งแทนเงินสดที่ออกโดยที่ทำการไปรษณีย์ซึ่งในบางประเทศถือเป็นตราสารทางการเงินที่สามารถขึ้นเงินกับธนาคารหรือที่ทำการไปรษณีย์ได้, เล็ตเตอร์ออฟเครดิต (Letter of Credit) หรือตราสารที่ได้รับการรับรองจากธนาคารพาณิชย์ในการชำระราคาสินค้าที่สั่งซื้อหรือนำเข้า หรือสินเชื่อในการนำเข้าสินค้าเพื่อนำไปจำหน่ายก่อน โดยให้ธนาคารออกเป็นหนังสือสัญญารับรองและรับรองการชำระราคาค่าสินค้าแทนผู้สั่งซื้อสินค้า (Trust Receipt) หรือการชำระเงินผ่านสื่อทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นการโอนหักบัญชีเงินฝาก, การชำระผ่านบัตรเครดิต, การชำระผ่านบัตรที่มีแถบแม่เหล็กหรือบัตรอิเล็กทรอนิกส์ ซึ่งรูปแบบการชำระเงินทางอิเล็กทรอนิกส์เป็นรูปแบบการชำระเงินที่ได้นำเทคโนโลยีทางคอมพิวเตอร์เข้ามาพัฒนาระบบให้มีคุณลักษณะ เพื่อรองรับการทำธุรกรรมทางการเงิน การธนาคารพาณิชย์ รวมถึงพาณิชย์อิเล็กทรอนิกส์ที่กำลังได้รับ

ความนิยม และขยายเครือข่ายคลอบคลุมการค้าขายระหว่างประเทศทั่วโลก ดังนั้นหากพิจารณาถึงวิวัฒนาการของระบบการชำระเงินในประเทศไทยสามารถแบ่งออกได้เป็น 3 ประเภท ดังนี้

2.2.2.1 ระบบการชำระเงินโดยใช้เงินสด (Cash Payment)

เงินสดเป็นสื่อกลางที่ได้รับความนิยมสูงสุดในการชำระราคาค่าสินค้าหรือค่าบริการต่างๆ อันเป็นผลเนื่องมาจากการทำธุรกรรมทางการค้า การพาณิชย์ หรือธุรกรรมทางการเงินการธนาคาร ด้วยเงินมีลักษณะที่มีมูลค่าชี้วัดและมีหน่วยราคาที่แน่นอน จึงเป็นสื่อกลางที่ได้รับการยอมรับกันโดยทั่วไป และสามารถใช้เป็นสื่อกลางในการชำระเงินระหว่างกันได้ทั่วโลก เงินสดจึงเป็นสื่อกลางในการชำระเงินพื้นฐานที่สามารถใช้เป็นดัชนีวัดอำนาจซื้อของประชาชน หรือสภาพเศรษฐกิจ สถานภาพทางการเงินการธนาคารของประเทศได้

ในปัจจุบันเงินสดในประเทศไทยประกอบด้วย ธนบัตร และเหรียญกษาปณ์ในรูปแบบต่างๆ โดยประเทศไทยเป็นสังคมที่ประชาชนส่วนใหญ่มีการใช้เงินสดในการชำระเงินมากกว่าประเทศอื่นๆ ดังจะเห็นได้จากสัดส่วนเฉลี่ยของการถือเงินสดของประชาชนในประเทศ ณ สิ้นปี ในช่วงปี 2536-2540 คิดเป็นร้อยละ 73 ในขณะที่ประเทศอื่นๆ มีอัตราการถือเงินสดของประชาชนในประเทศดังนี้ ประเทศฟิลิปปินส์มีอัตราร้อยละ 58 ประเทศสิงคโปร์มีอัตราร้อยละ 39 ประเทศสหรัฐอเมริกามีอัตราร้อยละ 31 ประเทศญี่ปุ่นและประเทศมาเลเซียมีอัตราร้อยละ 27[4] จึงถือได้ว่าส่วนใหญ่ระบบการชำระเงินด้วยเงินสดยังคงเป็นที่นิยมสูงสุดในการชำระเงินรายย่อย หรือในการชำระเงินของประชาชนส่วนใหญ่ในประเทศ

อย่างไรก็ตามในธุรกิจการค้า หรือการค้าขายระหว่างประเทศที่มีการขยายตัวเพิ่มมากขึ้นอย่างต่อเนื่องจึงทำให้ระบบการเงินการธนาคารของประเทศจำเป็นต้องมีปริมาณเงินสดหมุนเวียนในตลาดมากขึ้น ประกอบกับการจัดการเกี่ยวกับเงินสดล้วนแล้วแต่มีขั้นตอนที่ยุ่งยากและมีต้นทุนสูง ไม่ว่าจะเป็นการจัดพิมพ์ธนบัตร การตรวจนับ การคัดแยก การเก็บรักษา การขนส่ง การจัดการความชำรุดบกพร่องของเงิน รวมถึงต้องมีกระบวนการรักษาความปลอดภัยในการใช้เงินสดในระบบ ซึ่งล้วนแล้วแต่เป็นภาระและอุปสรรคต่อการดำเนินธุรกิจและการขยายตัวทางเศรษฐกิจของประเทศอย่างยิ่ง ดังนั้นจึงได้มีการพัฒนาสื่อการชำระเงินประเภท

---

[4] ธนาคารแห่งประเทศไทย, ระบบการชำระเงินในประเทศไทย, (กรุงเทพมหานคร : สายระบบการชำระเงิน ธนาคารแห่งประเทศไทย, 2542), หน้า 19-22.

อื่นๆ ขึ้นมาแทนเงินสด เพื่อให้การทำธุรกิจหรือธุรกรรมการซื้อขายสินค้าและบริการมีความสะดวกมากยิ่งขึ้น

2.2.2.2 การชำระเงินที่เป็นตราสาร (Paper-based Payments)

เมื่อมีการขยายตัวทางเศรษฐกิจ การชำระมูลค่าราคาสินค้าและบริการต่างๆ ด้วยเงินสดขาดความสะดวกและความคล่องตัวในการส่งมอบ เป็นภาระในการรวบรวม ขนย้ายและเก็บรักษา มีความเสี่ยงต่อการสูญหาย การปลอมแปลงเงินตราหรือใช้เงินตราปลอมอย่างมาก ด้วยเหตุนี้จึงได้มีการพัฒนาให้ใช้ตราสารเป็นสื่อกลางในการชำระเงิน ได้แก่

- คำสั่งโอนเงินโดยผ่านทางโทรเลข ไปรษณีย์ หรือโทรศัพท์ทางไกล
- เอกสารแสดงสิทธิเรียกร้องเงินจากผู้สั่งจ่าย ได้แก่ ดร๊าฟท์ หรือ เช็ค ซึ่งเป็นตราสารที่บุคคลหนึ่งเรียกว่าผู้สั่งจ่าย สั่งโดยปราศจากเงื่อนไข หรือมีเงื่อนไขอย่างหนึ่งอย่างใดให้ธนาคารจ่ายเงินตามที่ระบุไว้ในดร๊าฟท์หรือเช็คนั้น โดยธนาคารที่ผู้รับประโยชน์ได้นำตราสารนั้นไปขึ้นเงินจะจ่ายเงินให้แก่บุคคลอีกคนหนึ่งที่เรียกว่า "ผู้รับเงินหรือผู้รับประโยชน์" โดยหักจากบัญชีกระแสรายวันหรือบัญชีเงินฝากของผู้สั่งจ่าย ทั้งนี้ดร๊าฟท์หรือเช็คดังกล่าวได้มีการพัฒนารูปแบบต่าง ๆ และเรียกแตกต่างกันไปตามเงื่อนไขแห่งตราสารนั้น ได้แก่ เช็ค, เช็คเดินทาง (Treveller's Cheque) , เช็คเงินสด (Cashier Cheque), เช็คของขวัญ (Gift Cheque) , ดร๊าฟท์ (Draft) หรือ ตราสารที่เป็นคำสั่งทางการเงิน (Money Order), ธนาณัติหรือตราสารที่ออกโดยที่ทำการไปรษณีย์ (Postal Order), หรือ Treasurer's Cheque ซึ่งเป็นเช็คที่ออกโดยหน่วยงานของรัฐบาลและส่งให้กระทรวงการคลังเป็นผู้จ่ายเงิน แต่ผู้รับประโยชน์อาจมาขายต่อธนาคารก็ได้ โดยธนาคารจะเรียกเก็บเงินจากผู้สั่งจ่ายก่อนหรือเรียกเก็บภายหลังก็ได้
- ตั๋วแลกเงินเป็นตราสารที่บุคคลหนึ่งเรียกว่า ผู้สั่งจ่าย สั่งให้บุคคลคนหนึ่งเรียกว่า ผู้จ่าย จ่ายเงินจำนวนที่แน่นอนหรือจ่ายตามคำสั่งของบุคคลอีกคนหนึ่งเรียกว่าผู้รับเงิน โดยตั๋วแลกเงินจะมีกำหนดเวลาที่แน่นอนและมีเงื่อนไขให้ใช้เงินเมื่อทวงถามหรือมีเงื่อนไขอื่นๆ ก็ได้
- ตั๋วสัญญาใช้เงิน เป็นตราสารที่บุคคลหนึ่งเรียกว่าผู้ออกให้คำมั่นสัญญาว่าจะจ่ายเงินจำนวนหนึ่งหรือจ่ายตามคำสั่งของบุคคลอีกคนหนึ่งเรียกว่าผู้รับเงินเมื่อครบกำหนดชำระ โดยจะกำหนดอัตราดอกเบี้ยหรือไม่ก็ได้

2.2.2.3 การชำระเงินที่ไม่เป็นตราสารหรือการชำระเงินทางอิเล็กทรอนิกส์ (Paperless Payment or Electronic Funds Transfer)

การชำระเงินทางอิเล็กทรอนิกส์เป็นการชำระเงิน การส่งมอบเงิน หรือการโอนเงินผ่านสื่อหรือคำสั่งทางระบบคอมพิวเตอร์ เครื่องเทอร์มินัล สื่อหรืออุปกรณ์ทางอิเล็กทรอนิกส์ โดยเป็นการพัฒนาวิธีการชำระเงินจากระบบตราสารมาสู่ระบบการให้บริการธนาคารอิเล็กทรอนิกส์ และทำงานภายใต้ระบบการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ระหว่างกัน (EDI : Electronic Data Interchange) ในปัจจุบันการชำระเงินที่ไม่เป็นตราสารหรือการชำระเงินทางอิเล็กทรอนิกส์ในรูปแบบใหม่ ๆ นั้นได้มีการพัฒนาและนำมาใช้ในประเทศไทย

โดยการชำระเงินทางอิเล็กทรอนิกส์สามารถแบ่งออกได้เป็นการชำระเงินผ่านระบบการชำระเงินรายใหญ่หรือระบบบาทเน็ต (BAHTNET) ซึ่งเป็นระบบการชำระเงินระหว่างธนาคารแห่งประเทศไทยกับธนาคารพาณิชย์หรือสถาบันการเงินอื่น ๆ ที่มีกิจการเช่นเดียวกับธนาคารพาณิชย์ หรือการชำระเงินผ่านระบบการชำระเงินลูกค้ารายย่อย ซึ่งเป็นระบบการชำระเงินทางอิเล็กทรอนิกส์ที่นิยมใช้อยู่ในปัจจุบัน ได้แก่การโอนเงินระหว่างบัญชีตามคำสั่งล่วงหน้า (Direct Debit/Direct Credit) หรือการชำระเงินผ่านบัตรที่มีแถบแม่เหล็กหรือบัตรพลาสติก ไม่ว่าจะเป็นบัตรเดบิตหรือบัตรเอทีเอ็ม (Debit Card/ATM Card) หรือบัตรเครดิต (Credit Card), บัตรชำระเงินล่วงหน้า (Prepaid Card) ยกตัวอย่างเช่น บัตรเติมเงิน บัตรโทรศัพท์, หรือการบริการทางการเงินการธนาคารผ่านสื่ออิเล็กทรอนิกส์อื่นๆ (Electronic Banking) เช่น การให้บริการธนาคารทางโทรศัพท์, การให้บริการธนาคารทางอินเทอร์เน็ต (Internet Banking) หรือการให้บริการชำระเงินผ่านโทรศัพท์เคลื่อนที่ เป็นต้น

2.2.3 ลักษณะของระบบการชำระเงินของระบบการเงินการธนาคารในประเทศไทย

ระบบการชำระเงินของประเทศไทยอยู่ภายใต้การกำกับดูแลและการควบคุมของธนาคารแห่งประเทศไทย ซึ่งเป็นผู้ทำหน้าที่ในการพัฒนาระบบ กำกับ ดูแลและควบคุมระบบการชำระเงินภายในประเทศทั้งหมด และมีวัตถุประสงค์ในการสร้างโครงสร้างพื้นฐานต่างๆ เพื่อรองรับการให้บริการทางการเงินของประเทศ และเสริมสร้างประสิทธิภาพของระบบการชำระเงินโดยรวม รวมทั้งลดความเสี่ยงต่างๆ ที่อาจเกิดขึ้นภายใต้ระบบชำระเงิน ซึ่งระบบการชำระเงินของประเทศไทยภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทยจึงสามารถแบ่งรูปแบบของระบบการชำระเงินได้เป็น 3 ประเภท กล่าวคือ

2.2.3.1 ระบบการชำระเงินรายใหญ่หรือระบบบาทเนต

ระบบบาทเนต (BAHTNET) เป็นระบบการชำระเงินรายใหญ่ระหว่างสถาบันการเงินผ่านบัญชีเงินฝากของธนาคารแห่งประเทศไทยซึ่งเป็นระบบการชำระเงินมูลค่าสูงด้วยระบบอิเล็กทรอนิกส์ ซึ่งธนาคารแห่งประเทศไทยจะเป็นผู้ให้บริการแก่ธนาคารและสถาบันการเงินสมาชิกซึ่งมีเงินฝากอยู่ที่ธนาคารแห่งประเทศไทย โดยการโอนเงินในบัญชีเงินฝากของตนไปเข้าบัญชีของธนาคารหรือสถาบันสมาชิกผ่านข่ายงานของคอมพิวเตอร์ออนไลน์ รวมถึงระบบบาทเนตยังมีบริการโอนเงินเพื่อบุคคลที่สามซึ่งทำให้ธนาคารสามารถให้บริการแก่ลูกค้าในการโอนเงินไปยังธนาคารอื่นเพื่อเข้าบัญชีของผู้รับไม่ว่าจะเป็นการให้บริการดังต่อไปนี้

- การโอนเงิน (Fund Transfer)
- การโอนเงินเพื่อบุคคลที่สาม (Third Party Fund Transfer)
- การสอบถามข้อมูล (Inquiry)
- การส่งข่าวสารระหว่างกัน (Bilateral Communication)
- การประกาศข้อความ (Message Broadcast)
- การโอนเงินเพื่อชำระดุล (Multilateral Fund Transfer – MFT)

ซึ่งในปัจจุบัน ธนาคารแห่งประเทศไทยมีการพัฒนาระบบดังกล่าวเป็นระบบบาทเนต 2 เพื่อนำมาให้บริการลูกค้าแทนระบบเดิม โดยหลักสำคัญของระบบบาทเนต 2 ได้แก่ การเพิ่มธุรกรรมการส่งมอบ และชำระราคาตราสารหนี้ภาครัฐแบบ Delivery Versus Payment-Real Time Gross Settlement (DVP-RTGS) และสามารถใช้วิธีส่งคำสั่งผ่านระบบคอมพิวเตอร์ออนไลน์โดยผ่านได้ 2 ช่องทางคือ เครือข่าย S.W.I.F.T. หรือ BOT Webstation ซึ่งกระบวนการดังกล่าวจะส่งผลทำให้การระบบการชำระเงินของประเทศสามารถดำเนินไปได้อย่างสะดวก และรวดเร็ว

2.2.3.2 ระบบการหักบัญชีเช็คระหว่างธนาคารด้วยอิเล็กทรอนิกส์ (ECS)

ระบบดังกล่าวเป็นเป็นการชำระหนี้ด้วยเช็คจะเข้าสู่ระบบการหักบัญชีเช็คด้วยวิธีการทางอิเล็กทรอนิกส์ (Electronic Cheque Clearing) โดยศูนย์หักบัญชีอิเล็กทรอนิกส์จะเป็นหน่วยงานในการทำการอ่านและคัดแยกเพื่อจัดทำดุลการหักบัญชีเช็ค และใช้ข้อมูลเช็คนั้นส่งผ่านทางอิเล็กทรอนิกส์ เพื่อให้ธนาคารผู้รับคำสั่งได้ดำเนินการหักบัญชีตามเช็คนั้นกระบวนการเรียกเก็บเงินตามเช็คต่างธนาคารด้วยวิธีการทางอิเล็กทรอนิกส์ โดยนำระบบคอมพิวเตอร์และ

เทคโนโลยีในการส่งข้อมูลผ่านเครือข่ายสื่อสารมาใช้ในการประมวลผล ก่อนการนำตัวเช็คมาแลกเปลี่ยนกันและธนาคารจะได้รับข้อมูลเช็คเพื่อนำไปตัดบัญชีลูกค้าในเย็นวันเดียวกัน

2.2.3.3 ระบบการชำระเงินรายย่อยระดับลูกค้า

การให้บริการทางการเงินประเภทนี้ทำให้ธนาคารสมาชิกสามารถให้บริการลูกค้าในการชำระเงินรายย่อยระหว่างธนาคารสมาชิก โดยการชำระเงินผ่านบัญชีของธนาคารต่างธนาคารได้ ไม่ว่าจะเป็นการชำระเงินด้วยวิธีอิเล็กทรอนิกส์ออนไลน์ (Financial Electronic Data Interchange : FEDI) ซึ่งระบบที่รองรับการชำระเงินในการเชื่อมต่อกับการทำธุรกิจ EDI แบบครบวงจร หรือระบบเรียกเก็บเงินแบบMedia Clearing ซึ่งเป็นระบบการเรียกเก็บเงินหรือการชำระเงินรายย่อยระหว่างลูกค้าที่มีบัญชีอยู่ต่างธนาคาร โดยมีข้อตกลงล่วงหน้า และมีงวดการชำระเงินที่แน่นอน และมีปริมาณรายการมากทำให้การดำเนินการส่งข้อมูลคำสั่งโอนเงินเพื่อการชำระเงินผ่นระบบเครือข่าย web technology หรือสื่ออิเล็กทรอนิกส์ เช่น เทปแม่เหล็ก แผ่นจานแม่เหล็ก ทำให้ผู้ใช้บริการได้รับเงินในวันที่รายการมีผลสมบูรณ์ได้ทันที เช่นการสั่งจ่ายเงินเดือนพนักงาน เงินปันผล เป็นต้น

2.2.4 การให้บริการทางการเงินของธนาคารพาณิชย์ในประเทศไทย

ธนาคารพาณิชย์เป็นสถาบันทางการเงินที่มีบทบาทสำคัญอย่างยิ่งในการทำหน้าที่เป็นสื่อกลางในการชำระเงินภายใต้ระบบการเงินการธนาคารของประเทศไทย ซึ่งการให้บริการทางการเงินของธนาคารพาณิชย์ดังกล่าวสามารถแบ่งตามรูปแบบของการให้บริการได้ ดังต่อไปนี้

1. การให้บริการด้านเงินฝาก

1.1.การให้บริการเงินฝากประเภทเงินฝากออมทรัพย์ กล่าวคือ การฝากเงินในบัญชีที่ไม่จำกัดจำนวนเงินการฝาก ไม่จำกัดระยะเวลาในการฝากเป็นประจำ และสามารถเบิกถอนได้ตลอดเวลา

1.2.การให้บริการเงินฝากประเภทเงินฝากกระแสรายวัน กล่าวคือ การฝากเงินในบัญชีประเภทที่ธนาคารจะจ่ายเงินคืนเมื่อมีการทวงถาม และบัญชีประเภทนี้จึงต้องใช้เช็คในการเบิกถอนและโอนเงินจากบัญชีธนาคาร ซึ่งสามารถระบุกำหนดระยะเวลาในการเบิกถอนล่วงหน้าได้ เพื่ออำนวยความสะดวกต่อธุรกิจการค้า

1.3.เงินฝากประจำ (Fixed deposit) หมายถึง การฝากเงินในบัญชีที่กำหนดระยะเวลาในการฝากเงิน และธนาคารจะจ่ายเงินคืนพร้อมดอกเบี้ยตามอัตราที่กำหนดเมื่อสิ้นกำหนดระยะเวลา โดยใช้สมุดคู่ฝากเป็นหลักฐานในการรับฝากเงิน

1.4.การให้บริการเงินฝากประจำ-ใบรับฝาก (TDR : TIME DEPOSIT RECEIPT) ซึ่งเป็นการฝากเงินในบัญชี ประเภทเงินฝากประจำ หากแต่ทว่าใช้ใบรับฝากเป็นหลักฐานในการรับฝากเงินแทนสมุดคู่ฝาก ซึ่งใบรับฝากเงินนั้นต้องระบุถึงกำหนดระยะเวลาในการฝากเงิน จำนวนเงินฝาก วันที่ฝาก อัตราดอกเบี้ย ระยะเวลาฝากให้ผู้ฝากเป็นหลักฐาน

1.5.การให้บริการเงินฝากที่ออกบัตรเงินฝากให้แก่ลูกค้า(NCD : NEGOTIABLE CERTIFICATE OF DEPOSIT) หมายถึง การให้บริการทางการเงินโดยใช้บัตรเงินฝาก ซึ่งเป็นตราสารที่ออกให้แก่ลูกค้าเป็นการเฉพาะเจาะจง และผู้ถือบัตรหรือตราสารนี้สามารถเปลี่ยนมือได้

1.6.การรับฝากบัญชีด้วยเงินต่างประเทศ หมายถึง การให้บริการรับฝากเงินตราต่างประเทศตามที่ธนาคารกำหนดไว้โดยเฉพาะ ได้แก่ เงินสกุล USD, DM, HKD, SGD, YEN, GBP, MYR ทั้งที่เป็นบัญชีออมทรัพย์และบัญชีเงินฝากประจำ

2. การให้บริการโอนเงินภายในประเทศ หมายถึง การให้บริการทางการเงิน โดยการโอนเงินผ่านสื่อทางอิเล็กทรอนิกส์เฉพาะการโอนเงินข้ามเครือข่ายภายในประเทศ ไม่ว่าจะเป็นการโอนเงินผ่านทางโทรศัพท์, การให้บริการโอนเงินผ่านระบบบาทเนต หรือการให้บริการโอนเงินผ่านระบบอินเทอร์เน็ต

3. การให้บริการด้านการค้าต่างประเทศ

3.1. การให้บริการแก่สินค้าขาเข้า

3.1.1. การเปิดเล็ตเตอร์ออฟเครดิต (LETTER OF CREDIT : L/C) คือ การขอ ซื้อเงินตราต่างประเทศโดยการเปิดเล็ตเตอร์ออฟเครดิต(L/C) ซึ่งเล็ตเตอร์ออฟเครดิต หรือL/C ถือเป็นตราสารที่ออกให้เพื่อรองรับการดำเนินธุรกิจนำเข้าและธุรกิจส่งออกสินค้า และเป็นตราสารที่ออกโดยธนาคารตามคำสั่งของผู้ซื้อหรือผู้สั่งนำเข้าสินค้า และเป็นการให้เครดิตแก่ผู้ขายหรือผู้ส่งออกว่าธนาคารผู้ออก L/C จะเป็นผู้รับผิดชอบในการชำระเงินราคาค่าสินค้าให้แทนผู้ซื้อหรือผู้สั่งนำเข้าสินค้าตามที่ระบุไว้ในเล็ตเตอร์ออฟเครดิต (L/C)

3.1.2. การให้สินเชื่อเพื่อการนำเข้า (TRUST RECEIPT : T/R) โดย หมายถึง หนังสือสัญญาชนิดหนึ่งที่ผู้สั่งสินค้าได้ขอสินเชื่อไว้ต่อธนาคาร เพื่อเป็น

การรับรองว่าผู้สั่งซื้อขอรับเอกสารประกอบการนำเข้าอย่างครบถ้วน และทำการส่งสินค้าออกไปจำหน่ายก่อนจึงการชำระเงินตามตั๋วแลกเงินนั้น ๆ

3.2. การให้บริการแก่สินค้าขาออก

3.2.1. บริการแจ้งเล็ตเตอร์ออฟเครดิตที่เปิดมาให้กับผู้ส่งออก หมายถึง การขอเปิดเล็ตเตอร์ออฟเครดิตเช่นเดียวกับในข้อ 3.1.1 แต่ธนาคารผู้เปิดเครดิตจะเป็นผู้ส่ง L/C มาให้ผู้ขายหรือผู้ส่งออกผ่านธนาคารตัวแทนในประเทศของผู้ส่งออก ซึ่งปัจจุบันมีวิธีการส่งหรือแจ้งแก่ผู้ส่งออกได้หลายวิธี ได้แก่ การแจ้งผ่านทางโทรสาร, โทรเลข, จดหมาย หรือการโอนเงินผ่านระบบสวิฟท์ (SWIFT)

3.2.2 บริการโอนเล็ตเตอร์ออฟเครดิต หมายถึง การโอนเล็ตเตอร์ออฟเครดิตที่ได้เปิดไว้เช่นเดียวกับในข้อ 3.1.1 โดยเป็นการโอนหรือการส่งมอบเล็ตเตอร์ออฟเครดิตให้แก่ผู้อื่น และเล็ตเตอร์ออฟเครดิตดังกล่าวนั้นผู้เปิดเครดิต L/C ต้องได้ระบุไว้ชัดเจนว่า "พึงโอนได้" และการโอนนั้นต้องจำกัดให้โอนได้เฉพาะธนาคารที่ได้ระบุไว้เท่านั้น

3.2.3 บริการเรียกเก็บเงินตามตั๋วสินค้าออก หมายถึง การให้บริการทางการเงินในการเรียกเก็บเงินจากผู้สั่งซื้อหรือผู้นำเข้า โดยการส่งใบเรียกเก็บไปให้แก่ผู้สั่งซื้อสินค้าหรือผู้นำเข้า ผ่านธนาคารตัวแทนในประเทศผู้ซื้อและให้ธนาคารดังกล่าวทำหน้าที่เรียกเก็บเงินจากผู้สั่งซื้อสินค้าอีกกรณีหนึ่ง

3.2.4 บริการรับซื้อตั๋วเงินสินค้าขาออกตามเล็ตเตอร์ออฟเครดิต (L/C) หมายถึง การให้บริการทางการเงินในการรับซื้อ L/C จากผู้ขายหรือผู้ส่งออก เพื่อการขอขึ้นเงินภายใต้เงื่อนไขและข้อตกลงต่างๆ ที่กำหนดไว้ L/C เท่านั้น

3.2.5 สินเชื่อแพ็คกิ้งเครดิต หมายถึง สินเชื่อที่ธนาคารพาณิชย์เพื่อการส่งออกและนำเข้าแห่งประเทศไทยได้ให้ความอนุเคราะห์ทางการเงินแก่ผู้ส่งออกและผู้ผลิตสินค้าดังกล่าว โดยนำ L/C เป็นประกันการชำระเงินค่าราคาสินค้าที่นำเข้าดังกล่าว ทั้งนี้เพื่อให้เป็นการส่งเสริมการส่งสินค้าไปจำหน่ายต่างประเทศ ไม่ว่าจะเป็นสินค้าเกษตรและสินค้าอุตสาหกรรม

3.3 การให้บริการด้านปริวรรตเงินตราต่างประเทศ

3.3.1 การโอนเงินต่างประเทศขาเข้า (INWARD REMITTANCE) หรือการโอนเงินต่างประเทศขาออก (OUTWARD REMITTANCE) หมายถึง การโอน

เงินผ่านระบบ DRAFT (DRAWN ON BANK IN BANGKOK) โดยใช้อัตราแลกเปลี่ยนระบบ BUYING SIGHT BILL หรือการโอนเงินผ่านระบบ SWIFT/TELEX ใช้ระบบ BUYING T/T โดยเมื่อธนาคารให้รับแจ้งให้โอนเงินจากต่างประเทศผ่านระบบที่กล่าวข้างต้น ธนาคารจะต้องทำหน้าที่แปลงเงินตราต่างประเทศให้เป็นเงินบาท และธนาคารจะจ่ายเงินดังกล่าวที่ให้โอนเงินไปให้แก่ผู้รับเงิน

3.3.2 การซื้อและขายเช็คเดินทาง (Traveller' s Cheque) หมายถึง การให้บริการของธนาคารในการรับซื้อและการขายเช็คเดินทางและเช็คเดินทาง หมายถึงตราสารแทนเงินตราที่ใช้แลกเงินสดซึ่งเป็นเงินตราต่างประเทศของประเทศนั้นๆ ได้โดยการใช้อัตราแลกเปลี่ยนเงินตราต่างประเทศเป็นพื้นฐานในการรับชำระเงินตามเช็คดังกล่าว โดยผู้ถือเช็คสามารถนำเช็คดังกล่าวไปขึ้นเงินต่อธนาคารในต่างประเทศ ซึ่งต้องลงลายมือชื่อต่อหน้าเจ้าหน้าที่ธนาคาร และต้องลงลายมือชื่อให้เหมือนกับลายมือชื่อที่ปรากฏในเช็ค

3.3.3 การซื้อขายเงินตราต่างประเทศ หมายถึงการให้บริการในการรับซื้อและการขายธนบัตรทุกสกุลที่มีระบุไว้ในอัตราแลกเปลี่ยนตามอัตราการซื้อ (BUYING RATE BANK NOTE) และอัตราการขาย (SELLING RATE BANK NOTE)

3.3.4 การรับซื้อเช็คต่างประเทศ (PERSONAL CHEQUE หรือ DRAFT) หมายถึงการให้บริการในการรับซื้อเช็คต่างประเทศ โดยลูกค้าจะต้องมีวงเงิน ซื้อลดตั๋ว B/P (BALANCE PURCHASE) หรือบัญชีเงินฝากธนาคารเป็นหลักฐานไว้กับธนาคาร และธนาคารจะรับซื้อโดยการเข้าบัญชีให้ลูกค้า แต่จะเบิกเงินจะทำได้เมื่อเช็คเรียกเก็บเงินได้เท่านั้น โดยอัตราซื้อนั้นใช้อัตราการซื้อ ที่เรียกว่า BUYING RATE BANK NOTE

3.3.5 การขาย DRAFT ต่างประเทศ กล่าวคือ การให้บริการทางการเงินในการขาย Draft ให้แก่บุคคลที่มีวัตถุประสงค์ในการซื้อเป็นการเฉพาะ ไม่ว่าจะเป็นการซื้อ Draft เพื่อเดินทางไปต่างประเทศ, การศึกษา, ของขวัญ หรือการชำระราคาค่าสินค้าหรือค่าบริการบางประเภท เช่น ค่าหนังสือ ค่าสมาชิก เป็นต้น ทั้งนี้ต้องเป็นไปตามวงเงินที่ได้กำหนดไว้

3.3.6 การซื้อขายเงินในรูปเงินโอนระหว่างประเทศทางโทรเลข กล่าวคือ การให้บริการซื้อขายเงินตราต่างประเทศผ่านระบบโทรเลข ได้แก่ ระบบ SWIFT ซึ่งใช้เป็นเครือข่ายในการโอนเงินระหว่างประเทศ

3.3.7 SPOT TRANSACTION กล่าวคือ การให้บริการซื้อขายเงินตราต่างประเทศที่มีระยะเวลาในการส่งมอบภายในระยะเวลา 2 วันทำการ โดยอัตราในการซื้อขายดังกล่าว ธนาคารจะใช้อัตราการแลกเปลี่ยนเงินตราต่างประเทศเป็นหลักสำคัญในการพิจารณา

3.3.8 FORWORD TRANSACTION กล่าวคือ การให้บริการซื้อขายเงินตราต่างประเทศล่วงหน้าแก่ธุรกิจนี้เป็นการทำสัญญาซื้อขายเงินตราต่างประเทศล่วงหน้าและมีกำหนดระยะเวลา รวมทั้งคู่สัญญาทั้งสองฝ่ายมีภาระผูกพันให้ต้องปฏิบัติตามอัตราแลกเปลี่ยนและข้อกำหนดอื่น ๆ ที่ระบุในสัญญา เพื่อประโยชน์แก่การดำเนินธุรกิจที่สามารถรับรู้รายรับและรายจ่ายของธุรกิจในอนาคตได้

3.3.9 CURRENCY OPTION กล่าวคือ การให้บริการซื้อขายเงินตราต่างประเทศ โดยการทำข้อตกลงทำสัญญาให้สิทธิแก่ลูกค้าในการซื้อหรือขายเงินตราต่างประเทศ และการให้บริการดังกล่าวต้องอยู่ภายใต้อัตราสิทธิต่าง ๆ ที่ได้ตกลงกัน

3.3.10 FOREIGN EXCHANGE (SWAP) กล่าวคือ การให้บริการทางการเงินในการทำธุรกรรมการซื้อขายเงินตราต่างประเทศ ทั้งนี้ ธุรกรรมดังกล่าวมักมีวัตถุประสงค์ในการแลกเปลี่ยนเงินตราระหว่างประเทศ ดังนั้นการแลกเปลี่ยนเงินตราต่างประเทศดังกล่าว ธนาคารจึงต้องมีการรับประกันความเสี่ยงในการชำระเงิน หรือมีมาตรฐานในการซื้อขายเงินตราต่างประเทศที่มีความชัดเจน

3.3.11 INTEREST RATE PRODUCTS กล่าวคือ การให้บริการทางการเงินที่มีข้อตกลงในการชำระเงินระหว่างธนาคารและลูกค้า รวมทั้งมีการกำหนดอัตราดอกเบี้ยให้แตกต่างกัน ไม่ว่าจะเป็นสัญญาที่มีการกำหนดเงื่อนไขต่าง ๆ ที่เป็นที่ยอมรับกันโดยทั่วไป และกำหนดอัตราดอกเบี้ยในระยะแรกให้ใช้อัตราดอกเบี้ยคงที่ และเมื่อถึงกำหนดระยะเวลาหนึ่งให้ใช้อัตราลอยตัว หรือสัญญาอีกประเภทหนึ่งคือสัญญาที่มีข้อตกลงเรื่องอัตราดอกเบี้ยไว้ล่วงหน้า ซึ่งเป็นสัญญาที่สามารถป้องกันผลกระทบจากการ

เพิ่มขึ้นหรือการเปลี่ยนแปลงของอัตราดอกเบี้ยหรืออัตราแลกเปลี่ยนเงินตราต่างประเทศได้

3.4 การให้บริการกู้ยืมเงินและการให้สินเชื่อหมายถึง การให้เครดิตแก่ธุรกิจการค้าประเภทต่างๆ ในการขอใช้บริการกู้ยืมเงินและการขอสินเชื่อ ซึ่งการให้บริการกู้ยืมเงินหรือการให้สินเชื่อ หรือการให้เครดิตในการประกอบธุรกิจการค้านั้นมักมีรูปแบบการให้บริการที่แตกต่างกันไปตามลักษณะการให้บริการ หรือตามวัตถุประสงค์ของการให้บริการ ซึ่งมีรายละเอียดของการให้บริการกู้ยืมเงินหรือการให้สินเชื่อที่แตกต่างจากกัน ดังต่อไปนี้

3.4.1 การเปิดบัญชีเดินสะพัดประเภทเบิกเงินเกินบัญชี (OVERDRAFT: O.D.)

3.4.2 เงินให้กู้ยืมระยะสั้นตั๋วเงินในประเทศ(DOMESTIC BILLS – TIME BIBF)

3.4.2.1 เงินให้กู้ยืมของตั๋วเงินในประเทศมีกำหนดเวลา

3.4.2.2 เงินให้กู้ยืมของตั๋วเงินในประเทศมีกำหนดเวลา และเป็นเงินกู้ที่เป็นเงินตราต่างประเทศเพื่อชำระค่าสินค้านำเข้า

3.4.2.3 เงินให้กู้ยืมของตั๋วเงินในประเทศมีกำหนดเวลา และเป็นเงินกู้ที่เป็นเงินตราต่างประเทศ วงเงินประเภทแพ็คกิ้งเครดิตที่ออกภายใต้ L/C

3.4.2.4 การซื้อลดตั๋วเงินและตั๋วเงินเป็นเงินตราต่างประเทศ หมายถึง การให้บริการรับซื้อลดตั๋วเงินตามหนังสือสัญญาขายลดตั๋วสัญญาใช้เงิน

3.4.2.5 เงินให้กู้ยืมของตั๋วเงินในประเทศและชำระคืนเมื่อทวงถาม หมายถึง การให้บริการสินเชื่อที่มีการนำตั๋วเงินเป็นหลักประกันในการขอสินเชื่อ และมีกำหนดระยะเวลาในการชำระคืนก็ต่อเมื่อได้มีการทวงถามก่อน

3.4.2.6 การซื้อลดตั๋วเงินในประเทศ หมายถึง การให้บริการของธนาคารพาณิชย์ในการรับซื้อลดตั๋วเงินที่ออกโดยธนาคารพาณิชย์ภายในประเทศ ตามหนังสือสัญญาขายลดตั๋วสัญญาใช้เงิน

3.4.2.7 การซื้อลดตั๋วเงินที่ธนาคารรับรอง หมายถึง การให้บริการของธนาคารพาณิชย์ภายในประเทศไทยในการรับซื้อลดตั๋วเงินตามหนังสือสัญญาขายลดตั๋วสัญญาใช้เงิน ซึ่งตั๋วเงินดังกล่าวเป็นตั๋วเงินที่ธนาคารได้รับรองหรืออาวัลแล้ว

3.4.2.8 เงินให้กู้ยืมของตั๋วเงินสินค้าขาเข้าหมายถึง การให้บริการสินเชื่อที่มีการนำตั๋วเงินสินค้าขาเข้า หรือ เล็ตเตอร์ออฟเครดิต (L/C) เพื่อใช้เป็นหลักประกันในการขอสินเชื่อ

3.4.3 เงินให้กู้ยืมมีระยะยาวหมายถึง การให้บริการสินเชื่อหรือการให้เครดิตแก่ลูกค้า โดยเป็นเงินกู้ที่มีระยะเวลาในการผ่อนชำระ หรือระยะเวลาในการครบกำหนดเป็นระยะเวลานาน

3.4.4 การเปิด DL/C หมายถึง การให้บริการสินเชื่อ หรือการให้ใช้เครดิตของลูกค้าในการสั่งซื้อสินค้า และสร้างความมั่นใจให้แก่ผู้ขาย โดยธนาคารเป็นผู้รับรองการจ่ายเงินค่าสินค้าที่ได้นำเข้ามาภายในประเทศ หรือเป็นการให้เครดิตแก่ลูกค้าในการรับชำระเงินจากธนาคารตามใบสั่งซื้อ

3.4.5 การขายช่วงลดตั๋วเงิน หมายถึง การให้บริการสินเชื่อระยะสั้นที่ให้การสนับสนุนธุรกิจการค้าบางประเภท และเป็นทุนหมุนเวียนในการธุรกิจการค้าและผู้ประกอบการนั้น ทั้งนี้ผู้ประกอบการดังกล่าวต้องได้รับการอนุมัติวงเงินจากธนาคารแห่งประเทศไทยในการยินยอมให้ได้สินเชื่อระยะสั้นหรือเครดิตดังกล่าว ซึ่งปัจจุบันผู้ประกอบการที่ได้รับการอนุญาตจากธนาคารแห่งประเทศไทยให้ได้รับวงเงินหรือสินเชื่อระยะสั้นดังกล่าวได้แก่ ผู้ประกอบการค้าทางด้านพืชผลเกษตร, ผู้ประกอบการค้าทางด้านอุตสาหกรรม, ผู้ประกอบการทางด้านยางพารา และผู้ประกอบการทางด้านการเลี้ยงสัตว์

3.4.6 สินเชื่อธุรกิจ เป็นการให้บริการสินเชื่อแก่ธุรกิจที่มีขนาดใหญ่และขนาดปานกลางเพื่อเป็นการสนับสนุนธุรกิจการค้า ธุรกิจการพาณิชย์ให้สามารถทำกำไรและมีอัตราการเจริญเติบโตไปได้เป็นอย่างดี

3.4.7 การออกหนังสือค้ำประกัน หมายถึง การให้บริการของธนาคารพาณิชย์ในการค้ำประกันให้แก่บุคคลที่ 3 เพื่อการรับรองการทำนิติกรรมประเภทต่าง ๆ โดยออกมาในรูปแบบของหนังสือสัญญาค้ำประกัน

3.4.8 การรับรองและอาวัลตั๋วเงิน หมายถึง การให้บริการของธนาคารพาณิชย์ในการรับรองหรือการรับประกันการชำระเงินตามตั๋วแลกเงินอันเป็นการทำให้ตั๋วแลกเงินดังกล่าวมีความน่าเชื่อถือต่อธุรกิจการค้า การธนาคารพาณิชย์มากขึ้น

3.4.9 การให้บริการจัดหาแหล่งเงินกู้จากต่างประเทศให้กับธุรกิจ หมายถึง การให้บริการของธนาคารพาณิชย์ในการรับฝากหรือการกู้ยืมเงินตราต่างประเทศจากบุคคลธรรมดาหรือนิติบุคคลในต่างประเทศ หรือสาขาของ

ธนาคารพาณิชย์ในต่างประเทศที่จัดตั้งขึ้นในประเทศไทย หรือสาขาธนาคารพาณิชย์ในต่างประเทศตลอดจนนิติบุคคลอื่นตามที่ธนาคารแห่งประเทศไทยเป็นผู้กำหนดเพื่อให้กู้ยืมเงินแก่บุคคลหรือนิติบุคคลภายในประเทศ หรือการให้บริการของธนาคารพาณิชย์ในการรับฝาก หรือการกู้ยืมเงินตราต่างประเทศ เพื่อให้กู้ยืมสินหรือให้เครดิตไปยังต่างประเทศ ไม่ว่าจะเป็นการรับฝากหรือการให้กู้ยืมเงินตราต่างประเทศในรูปแบบของสกุลเงินตราต่างประเทศหรือสกุลเงินบาท

3.5 บริการพิเศษอื่นๆ ที่สามารถชำระผ่านระบบการธนาคารพาณิชย์

3.5.1 บริการชำระค่าสาธารณูปโภค เพื่อเป็นการอำนวยความสะดวกให้แก่ลูกค้าในการรับชำระเงินค่าสาธารณูปโภค ไม่ว่าจะเป็นการรับชำระค่าไฟฟ้า ค่าน้ำประปา หรือค่าโทรศัพท์

3.5.2 บริการโอนเงินตามคำสั่งลูกค้า(STANDING ORDER) หมายถึง การให้บริการโอนเงินไปยังผู้รับเงิน โดยการโอนผ่านการหักบัญชีธนาคารตามวันและเวลาที่ได้กำหนดตามคำสั่งของลูกค้า ไม่ว่าจะเป็นการโอนเงินระหว่างบัญชีภายในธนาคารเดียวกัน หรือการโอนเงินระหว่างบัญชีต่างธนาคารก็ได้

3.5.3 บริการตัดบัญชีชำระค่าบัตรเครดิต หมายถึง การให้บริการทางการเงินของธนาคารพาณิชย์ร่วมกับบริษัทเจ้าของบัตรเครดิตในการรับชำระค่าใช้จ่ายต่าง ๆ บัตรเครดิตผ่านการหักบัญชีธนาคารของลูกค้า ซึ่งค่าใช้จ่ายต่างๆ ที่หักผ่านบัญชีธนาคารดังกล่าวจะถูกหักตามจำนวนและกำหนดเวลาที่บริษัทเจ้าของบัตรเครดิตเป็นผู้กำหนด ทั้งนี้ย่อมอยู่ภายใต้การควบคุมของธนาคารแห่งประเทศไทยด้วย

3.5.4 บริการชำระค่าเบี้ยประกัน หมายถึง การให้บริการทางการเงินของธนาคารพาณิชย์ในการรับชำระค่าเบี้ยประกันต่าง ๆ โดยการหักบัญชีธนาคารตามกำหนดเวลาและจำนวนเงินที่บริษัทประกันภัยเป็นผู้กำหนด

3.5.5 บริการจ่ายเงินเดือนเข้าบัญชีพนักงานบริษัทหมายถึง การให้บริการทางการเงินของธนาคารในการรับจ่ายเงินเดือนให้แก่พนักงานของบริษัทตามกำหนดการจ่ายเงินเดือนที่บริษัทได้แจ้งไว้ โดยบริษัทจะต้องส่งเช็คมายังธนาคารพร้อมรายงานเงินเดือนของพนักงานในการเป็นฐานข้อมูลและเป็นการอำนวยความสะดวกในการจ่ายเงินเดือนให้แก่พนักงานของบริษัทต่อไป

3.5.6 เช็คสั่งจ่ายของธนาคาร หมายถึง ตราสารที่ออกโดยธนาคาร เพื่อการชำระเงินแทนการชำระเงินด้วยเงินสด

3.5.7 การให้บริการผ่านบัตรเงินสด (CASH CARD) หมายถึง การให้บริการเงินสดของธนาคารพาณิชย์ โดยผู้ถือบัตรเดบิตหรือบัตรเอทีเอ็มใช้บัตรอิเล็กทรอนิกส์ดังกล่าวในการฝาก ถอน หรือโอนเงินผ่านเครื่องรับฝากและถอนเงินอัตโนมัติ (เครื่องเอทีเอ็ม)

3.5.8 การให้บริการตู้นิรภัย หมายถึง การให้บริการของธนาคารพาณิชย์ในการเช่าตู้นิรภัยเพื่อเก็บรักษาทรัพย์สินที่มีค่า หรือเอกสารสำคัญให้ปลอดภัยจากอัคคีภัย การโจรกรรม

3.5.9 การออกหนังสือรับรองฐานะทางการเงิน หมายถึง การให้บริการของธนาคารพาณิชย์ในการรับรองฐานะทางการเงินของลูกค้า ในกรณีการขอวีซ่าเพื่อเดินทางไปต่างประเทศ การศึกษาต่อในต่างประเทศ การยื่นขอประกันต่อศาล การทำบัตรภาษีศุลกากร หรือการทำบัตรเครดิต และอื่นๆ โดยธนาคารจะออกหนังสือรับรองฐานะทางการเงินตามยอดเงินของบัญชีเงินฝากของลูกค้า

3.5.10 การให้บริการรับชำระภาษี หมายถึง การให้บริการของธนาคารพาณิชย์ในการรับชำระค่าภาษีรถยนต์หรือรถจักรยานยนต์ หรือการรับชำระภาษีเงินได้บุคคลธรรมดาหรือนิติบุคคลเพื่อส่งให้กรมสรรพากร

3.5.11 การรับซื้อหน่วยลงทุนของกองทุนรวม หมายถึง การให้บริการของธนาคารพาณิชย์ในการเป็นตัวแทนการจำหน่ายหุ้นสามัญ หุ้นกู้ ตราสารหนี้ของกองทุนปิดหรือกองทุนเปิดของบริษัทหลักทรัพย์จัดการกองทุนรวม (บลจ.) ตามที่ธนาคารได้ประกาศไว้ผ่านธนาคารสาขาหรือให้หน่วยงานใดเป็นผู้รับผิดชอบ

3.5.12 การให้บริการด้านวาณิชธนกิจ หมายถึงการให้บริการของธนาคารพาณิชย์ในรูปแบบที่นอกเหนือไปจากการให้บริการตามปกติของธนาคาร ซึ่งอยู่ภายใต้การทำงานและการกำกับดูแลของฝ่ายวาณิชธนกิจของธนาคารพาณิชย์นั้นๆ ได้แก่ การจัดจำหน่ายและรับประกันการจัดจำหน่ายตราสารแห่งหนี้ การให้คำปรึกษาทางการเงิน หรือการร่วมปล่อยกู้กับผู้สนับสนุนทางการเงินรายอื่น หรือจัดหาแหล่งเงินกู้

2.3 การโอนเงินทางอิเล็กทรอนิกส์ภายใต้ระบบการเงินการธนาคารของประเทศไทย

ด้วยระบบการเงินการธนาคารในปัจจุบันมีการขยายตัวอย่างรวดเร็ว และมีการพัฒนาทางด้านเทคโนโลยีคอมพิวเตอร์ให้เข้ามามีบทบาท และทำให้ระบบการชำระเงินทางการโอนเงินทางอิเล็กทรอนิกส์เป็นการให้บริการทางการเงินการธนาคารที่ได้รับความนิยมสูงสุด ภายใต้ระบบการชำระเงินในประเทศไทย ซึ่งหากกล่าวถึงคำนิยามของคำว่า การโอนเงินทางอิเล็กทรอนิกส์ หมายถึง การโอน เคลื่อนย้ายหรือส่งมอบเงินจากบุคคลหนึ่งไปยังอีกบุคคลหนึ่ง หรือจากที่หนึ่งไปยังอีกที่หนึ่ง โดยใช้คำสั่งหรือการป้อนข้อมูลผ่านเครื่องเทอร์มินัล เครื่องคอมพิวเตอร์ เครื่องประมวลผลข้อมูล อุปกรณ์หรือสื่อทางอิเล็กทรอนิกส์ ซึ่งเครื่องคอมพิวเตอร์ อุปกรณ์หรือสื่อทางอิเล็กทรอนิกส์ที่ได้รับคำสั่งจะทำหน้าที่แปลรหัสข้อมูลที่ได้รับ และหากเมื่ออ่านข้อมูลและรหัสที่ได้รับได้อย่างถูกต้องธนาคารพาณิชย์จะทำการอนุมัติให้โอน ส่งมอบ หรือเคลื่อนย้ายเงินเข้าหรือออกจากบัญชีได้ตามคำสั่งดังกล่าว

ซึ่งความหมายของคำว่า การโอนเงินทางอิเล็กทรอนิกส์ ซึ่งธนาคารแห่งประเทศไทยได้ให้ความหมายหรือคำจำกัดความของการโอนเงินทางอิเล็กทรอนิกส์ไว้ในหนังสือที่ ธปท.งก. 1230/2537 เรื่องหลักเกณฑ์การให้บริการโดยเงินทางอิเล็กทรอนิกส์ ฉบับวันที่5 กรกฎาคม 2537 กล่าวคือ

"การโอนเงินทางเครื่องอิเล็กทรอนิกส์" หมายถึง การโอนเงินที่กระทำผ่านเครื่องเทอร์มินัล หรืออุปกรณ์สื่อสารของอิเล็กทรอนิกส์ หรือเครื่องคอมพิวเตอร์ เพื่อส่งให้ธนาคารพาณิชย์โอนเงินเข้าหรือออกจากบัญชี เช่น การโอนเงินทางเครื่องเทอร์มินัลผ่านสำนักงานสาขาหรือสำนักงานของธนาคารพาณิชย์ การให้บริการเครื่องอิเล็กทรอนิกส์ที่ใช้ในการฝากและถอนเงิน (ATM) การโอนเงิน ณ จุดขาย (POS)บริการธนาคารในสำนักงาน (Office Banking) และการบริการธนาคารทางโทรศัพท์ (Telebanking) เป็นต้น ซึ่งจะถือว่าการโอนเงินจะเสร็จสิ้นสมบูรณ์ก็ต่อเมื่อผู้รับโอนหรือผู้รับประโยชน์ได้รับเงินสด หรือได้รับเครดิตบัญชีให้ครบถ้วนตามจำนวนเงินที่โอนเข้าบัญชีของผู้รับเงินจากธนาคารผู้โอนหรือธนาคารผู้รับโอนเรียบร้อยแล้ว และผู้รับโอนสามารถใช้เงินนั้นได้[5]

หากพิจารณาถึงคำนิยามของคำว่า "การโอนเงินทางอิเล็กทรอนิกส์" ตามพระราชบัญญัติโอนเงินทางเครื่องอิเล็กทรอนิกส์ ค.ศ.1978 (Electronic Fund Transfer Act 1978) แห่ง

---

[5]"หนังสือที่ ธปท.งก. 1230/2537เรื่องหลักเกณฑ์การให้บริการโดยเงินทางอิเล็กทรอนิกส์" ธนาคารแห่งประเทศไทย,(ม.ป.ท.),(2537).

ประเทศสหรัฐอเมริกาได้ให้คำจำกัดความคำว่า "การโอนเงินทางอิเล็กทรอนิกส์" ตามมาตรา 1693a (6) กล่าวคือ

การโอนเงินโดยเครื่องอิเล็กทรอนิกส์ หมายถึง การโอนเงินใด ๆ นอกเหนือไปจากการโอนเงินด้วยเช็ค, ดร๊าฟท์ หรือตราสารอื่นที่สามารถโอนได้ทำนองเดียวกัน โดยทางอิเล็กทรอนิกส์ ทางโทรศัพท์ หรือคอมพิวเตอร์ หรือแถบแม่เหล็กตามคำสั่งหรือการอนุญาตให้หักบัญชีหรือเครดิตบัญชี ทั้งนี้ ให้รวมถึงคำสั่งโอนเงิน ณ จุดขาย การโอนด้วยเครื่องATM การฝากหรือถอนเงินโดยตรง และการโอนทางโทรศัพท์ แต่ไม่รวมถึง

(A) การรับรองเช็คใด ๆ หรือการบริการที่ไม่เกี่ยวกับการหักบัญชีหรือให้เครดิตโดยตรงต่อบัญชีของผู้ใช้บริการ

(B) การโอนเงินใดๆ นอกเหนือจากการดำเนินการโดยสำนักหักบัญชีอัตโนมัติของสถาบันการเงินแก่ผู้ใช้บริการโดยวิธีการโอนเงินของธนาคารกลางหรือสถาบันรับฝากอื่นๆ ที่มิได้มีไว้เพื่อการโอนเงินแก่ผู้ใช้บริการ

(C) การโอนเงินใดที่ไม่ใช่เพื่อการซื้อหรือขายหลักทรัพย์หรือเครื่องอุปโภคผ่านตัวแทนที่จดทะเบียนกับตลาดหลักทรัพย์

(D) การโอนโดยอัตโนมัติจากบัญชีออมทรัพย์หรือจากบัญชีเผื่อเรียก ตามข้อตกลงระหว่างผู้ใช้บริการและสถาบันการเงินเพื่อสินเชื่อในบัญชีของผู้บริโภค หรือ

(E) การโอนเงินใดๆ โดยทางโทรศัพท์ระหว่างผู้ใช้บริการและเจ้าหน้าที่ หรือโดยพนักงานของสถาบันการเงิน ซึ่งเป็นไปตามแผนอันตกลงกันไว้แล้วและอยู่ภายใต้การโอนเป็นช่วงๆ หรือการโอนที่ไม่มีการไตร่ตรองมาก่อนกับได้ตกลงตามระเบียบของคณะกรรมการ[6]

---

[6] Electronic Fund Transfer Act 1978., sec.1693a (6).

The term "electronic fund transfer" means any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account. Such term includes, but is not limited to, point-of-sale transfers, automated teller machine transactions, direct deposits or withdrawals of funds, and transfers initiated by telephone. Such term does not include –

(A) any check guarantee or authorization service which does not directly result in a debit or credit to a consumer's account;

2.3.1 ความสำคัญของการโอนเงินทางอิเล็กทรอนิกส์

การโอนเงินทางอิเล็กทรอนิกส์ (Electronic Fund Transfer หรือ EFT) เป็นการนำเอาความก้าวหน้าของเทคโนโลยีคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศเข้ามาพัฒนาสื่อการชำระเงินทำให้สามารถชำระเงินได้อย่างสะดวก รวดเร็ว มีความทันสมัย ลดภาระขั้นตอนที่ยุ่งยากหรือซ้ำซ้อนในการชำระเงิน ลดการใช้กระดาษ หรือตราสารต่างๆ ซึ่งเป็นการเพิ่มความรวดเร็วในธุรกิจการค้า ลดความผิดพลาดจากการทำงานของมนุษย์ ประกอบกับการโอนเงินทางอิเล็กทรอนิกส์ยังเป็นการเสริมสร้างประสิทธิภาพและศักยภาพในการแข่งขันระหว่างธนาคารพาณิชย์และสถาบันการเงินต่างๆ ในการให้บริการทางการเงินหรือธุรกรรมทางการพาณิชย์อิเล็กทรอนิกส์ให้แก่แวดวงธุรกิจการค้าได้อย่างกว้างขวาง ไม่ว่าจะเป็นการเชื่อมโยงเครือข่ายการทำธุรกรรมทางการเงินภายในประเทศและธุรกรรมทางการเงินระหว่างประเทศให้สามารถเชื่อมโยงระหว่างกันได้ทั่วโลก

ด้วยเหตุนี้ การโอนเงินทางอิเล็กทรอนิกส์จึงมีความสำคัญต่อระบบการเงินการธนาคาร ระบบเศรษฐกิจ ธุรกิจการค้า และการธนาคารพาณิชย์ของประเทศ ด้วยเหตุว่าธนาคารพาณิชย์เปรียบเสมือนศูนย์กลางทางการเงินการธนาคาร และศูนย์กลางของธุรกิจการค้า

(B) any transfer of funds, other than those processed by automated clearinghouse, made by a financial institution on behalf of a consumer by means of a service that transfers funds held at either Federal Reserve banks or other depository institutions and which is not designed primarily to transfer funds on behalf of a consumer;

(C) any transaction the primary purpose of which is the purchase or sale of securities or commodities through a broker-dealer registered with or regulated by the Securities and Exchange Commission;

(D) any automatic transfer from a savings account to a demand deposit account pursuant to an agreement between a consumer and a financial institution for the purpose of covering an overdraft or maintaining an agreed upon minimum balance in the consumer's demand deposit account; or

(E) any transfer of funds which is initiated by a telephone conversation between a consumer and an officer or employee of a financial institution which is not pursuant to a prearranged plan and under which periodic or recurring transfers are not contemplated; as determined under regulations of the Board;

ทั้งธุรกิจภายในประเทศและธุรกิจระหว่างประเทศ ดังนั้นการให้บริการของธนาคารพาณิชย์จึงต้องมีความน่าเชื่อถือและสามารถสร้างความไว้วางใจให้แก่ลูกค้าไม่ว่าจะเป็นบุคคลธรรมดาหรือนิติบุคคล เพื่อส่งผลให้ระบบการชำระเงินภายใต้ระบบการเงินการธนาคารของประเทศมีความมั่นคง และสามารถสร้างเสถียรภาพทางการเงินและเสถียรภาพทางเศรษฐกิจให้แก่ประเทศได้

นอกจากนั้น การโอนเงินทางอิเล็กทรอนิกส์ยังมีบทบาทอย่างมากต่อระบบการเงินการธนาคารซึ่งเป็นไปตามการประกาศรับพันธะตามมาตรา 8 แห่งข้อตกลงของกองทุนการเงินระหว่างประเทศ ซึ่งแต่เดิมด้วยภาวะหลังสงครามมหาเอเชียบูรพาประเทศไทยมีสภาพเศรษฐกิจตกต่ำ ฐานะทางการเงินของประเทศอยู่ในระยะที่ไม่มั่นคง และประเทศไทยอยู่ในสภาวะที่ขาดแคลนเงินตราต่างประเทศเป็นอย่างมาก ประกอบกับเงินกองทุนสำรองต่างประเทศมีไม่มากนัก ดังนั้นประเทศไทยจึงจำเป็นต้องมีกฎหมายในการควบคุมการแลกเปลี่ยนเงินตราต่างประเทศ(ควบคุมการปริวรรตเงินตรา) เพื่อควบคุมปริมาณเงินสดภายในประเทศและให้เงินตราภายในประเทศอยู่ในสภาวะที่มั่นคงมากขึ้น ดังนั้นจึงได้มีการประกาศกฎหมายควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485 ขึ้นในประเทศไทย

จนกระทั่งในปี พ.ศ.2530 สภาวะทางการเงินภายในประเทศไทยมีความมั่นคงมากขึ้นและสถานภาพทางเศรษฐกิจมีการเจริญเติบโตที่เป็นไปอย่างรวดเร็ว ประกอบกับประเทศไทยเป็นประเทศภาคีสมาชิกของกองทุนการเงินระหว่างประเทศ ดังนั้นกระทรวงการคลังและธนาคารแห่งประเทศไทยจึงมีความเห็นร่วมกัน ในการประกาศยอมรับพันธะข้อผูกพันตามมาตรา 8 แห่งข้อตกลงของกองทุนการเงินระหว่างประเทศ เมื่อวันที่ 21 พฤษภาคม พ.ศ. 2533 ซึ่งมีสาระสำคัญดังต่อไปนี้

1. การห้ามข้อจำกัดในการชำระเงินหรือโอนเงินเพื่อธุรกิจเดินสะพัดระหว่างประเทศ
2. การห้ามการบังคับใช้สัญญาแลกเปลี่ยนทางการเงินอื่นที่ขัดกับระเบียบการควบคุมการแลกเปลี่ยนเงินของประเทศสมาชิกอื่น
3. การห้ามวิธีปฏิบัติทางการเงินที่ลำเอียงหรือการใช้อัตราแลกเปลี่ยนหลายอัตราโดยไม่ได้รับความเห็นชอบจากกองทุนการเงินระหว่างประเทศ

ซึ่งหากพิจารณาถึงหลักการและสาระสำคัญของประกาศแห่งข้อตกลงของกองทุนการเงินระหว่างประเทศ ตามมาตรา 8 ดังกล่าวจะเห็นได้ว่ามีหลักการสำคัญอยู่ 2 กรณี กล่าวคือ การมุ่งเน้นให้ตลาดเงินตราต่างประเทศดำเนินไปได้อย่างเสรี และลดข้อจำกัดต่างๆ ในการโอนเงินระหว่างประเทศ รวมทั้งการสนับสนุนให้มีการเปิดเผยข้อมูลทางการโอนเงินทางอิเล็กทรอนิกส์

ตามที่กองทุนระหว่างประเทศ และจึงเป็นสาเหตุสำคัญอีกประการหนึ่งที่ทำให้การโอนเงินทางอิเล็กทรอนิกส์มีบทบาทสำคัญอย่างยิ่งต่อระบบการเงินการธนาคารในประเทศไทย

2.3.2 ลักษณะการโอนเงินทางอิเล็กทรอนิกส์

การโอนเงินทางอิเล็กทรอนิกส์เป็นธุรกรรมทางการเงินการธนาคาร ที่ได้รับความนิยมอย่างมากในปัจจุบัน โดยการใช้เทคโนโลยีคอมพิวเตอร์ อุปกรณ์หรือเครื่องมือทางอิเล็กทรอนิกส์ผ่านธนาคารพาณิชย์ หรือสถาบันการเงินอื่นใด ๆ ที่ได้รับอนุญาตจากธนาคารแห่งประเทศไทยให้ประกอบกิจการลักษณะเดียวกับธนาคารพาณิชย์ เพื่อใช้ระบบอิเล็กทรอนิกส์เป็นสื่อกลางในการโอนเงินทางอิเล็กทรอนิกส์ภายใต้ระบบการชำระเงินในประเทศไทย

รูปแบบการโอนเงินทางอิเล็กทรอนิกส์ที่ใช้อยู่ในปัจจุบัน ได้แก่ การโอนเงินทางอิเล็กทรอนิกส์รายใหญ่หรือระบบบาทเนต ซึ่งเป็นการโอนเงินระหว่างธนาคาร หรือสถาบันการเงินด้วยการโอนบัญชีเงินฝากที่ธนาคารแห่งประเทศไทย(Bank of Thailand Automated High-Value Network - BAHTNET) ซึ่งระบบบาทเนตที่ใช้อยู่ในปัจจุบันเป็นระบบบาทเนต 2 (BAHTNET 2) และระบบการชำระดุลรายย่อยระดับลูกค้าที่ให้บริการทั้งภายในประเทศ และการชำระเงินระหว่างประเทศ

2.3.3 รูปแบบ ลักษณะของการโอนเงินทางอิเล็กทรอนิกส์ในประเทศไทย

การโอนเงินทางอิเล็กทรอนิกส์ที่ใช้อยู่ในปัจจุบันสามารถแบ่งตามลักษณะของการโอนเงินได้ดังนี้

1. การโอนเงินทางอิเล็กทรอนิกส์ผ่านระบบชำระเงินรายใหญ่หรือการโอนเงินทางอิเล็กทรอนิกส์ระหว่างธนาคารหรือสถาบันการเงิน

1.1. การโอนเงินทางอิเล็กทรอนิกส์ผ่านระบบบาทเนต (BAHTNET) เป็นระบบการโอนเงินรายใหญ่ระหว่างธนาคารหรือสถาบันการเงินสมาชิก ผ่านบัญชีเงินฝากของธนาคารแห่งประเทศไทย ซึ่งธนาคารหรือสมาชิกได้มีบัญชีกับธนาคารแห่งประเทศไทยไว้โดยผ่านข่ายงานของคอมพิวเตอร์ออนไลน์ของธนาคารแห่งประเทศไทย ซึ่งในปัจจุบันธนาคารแห่งประเทศไทยมีการพัฒนาระบบบาทเนตเป็นระบบบาทเนต 2 เพื่อนำมาให้บริการลูกค้าแทนระบบเดิม โดยหลักสำคัญของระบบบาทเนต 2 คือ การเพิ่มธุรกรรมการส่งมอบและชำระราคาตราสาร

หนี้ภาครัฐแบบ Delivery Versus Payment-Real Time Gross Settlement (DVP-RTGS) นอกจากนั้นระบบบาทเนต 2 นี้ยังสามารถให้บริการโดยใช้วิธีส่งคำสั่งผ่านระบบคอมพิวเตอร์ออนไลน์โดยผ่านได้ 2 ช่องทางคือ เครือข่าย S.W.I.F.T. หรือ BOT Webstation ซึ่งส่งผลทำให้การธุรกรรมการโอนเงินทางอิเล็กทรอนิกส์สามารถดำเนินไปได้อย่างสะดวกและรวดเร็ว ส่วนหากเป็นการชำระหนี้ด้วยเช็คจะเข้าสู่ระบบการหักบัญชีเช็คด้วยวิธีการทางอิเล็กทรอนิกส์ (Electronic Cheque Clearing) โดยศูนย์หักบัญชีอิเล็กทรอนิกส์จะเป็นหน่วยงานในการทำการอ่านและคัดแยกเพื่อจัดทำดุลการหักบัญชีเช็ค และใช้ข้อมูลเช็คนั้นส่งผ่านทางอิเล็กทรอนิกส์ เพื่อให้ธนาคารผู้รับคำสั่งได้ดำเนินการหักบัญชีตามเช็คนั้น

1.2. ระบบ Media Clearing เป็นระบบการเรียกเก็บเงิน หรือระบบการโอนเงินรายย่อยข้ามธนาคารพาณิชย์สำหรับรายจ่ายประจำโดยมีข้อตกลงล่วงหน้า ซึ่งทำงานในระบบ off-line ดังนั้นการติดต่อทำธุรกรรมต่างๆ จะต้องติดต่อไว้ล่วงหน้าก่อน 1-7 วันทำการ เช่น การจ่ายเงินเดือนพนักงาน การชำระเงินค่าสาธารณูปโภคต่างๆ โดยธนาคารสมาชิกจะทำการผ่านศูนย์หักบัญชีอิเล็กทรอนิกส์ เมื่อศูนย์หักบัญชีอิเล็กทรอนิกส์ได้ประมวลผล และจัดทำดุลชำระบัญชี เมื่อทำการชำระดุลเรียบร้อย ศูนย์หักบัญชี ฯ จะส่งข้อมูลผ่านสื่ออิเล็กทรอนิกส์เพื่อให้ธนาคารสมาชิกนำไปประมวลผลและบันทึกบัญชีลูกค้าของตนต่อไป การให้บริการทางการเงินประเภทนี้ทำให้ธนาคารสมาชิกสามารถให้บริการลูกค้าในการโอนเงินรายย่อย โดยทั้งผู้โอนและผู้รับโอนสามารถทำโอนเงินผ่านบัญชีของธนาคารต่างธนาคารได้

1.3 ระบบการหักบัญชีเช็คระหว่างธนาคารด้วยอิเล็กทรอนิกส์ (ECS) เป็นกระบวนการเรียกเก็บเงินตามเช็คต่างธนาคารด้วยวิธีการทางอิเล็กทรอนิกส์โดยนำระบบคอมพิวเตอร์และเทคโนโลยีในการส่งข้อมูลผ่านเครือข่ายสื่อสารมาใช้ในการประมวลผลก่อนการนำตัวเช็คมาแลกเปลี่ยนกันและธนาคารจะได้รับข้อมูลเช็คเพื่อนำไปตัดบัญชีลูกค้าในเย็นวันเดียวกันนั้น

2. การโอนเงินทางอิเล็กทรอนิกส์ผ่านระบบชำระเงินรายย่อยระดับลูกค้า

หากพิจารณาถึงระบบการชำระเงินรายย่อย หรือระบบการชำระเงินระหว่างธนาคารพาณิชย์หรือสถาบันทางการเงินสมาชิกเป็นส่วนหนึ่งที่สำคัญในการให้บริการทางการเงินการธนาคารภายใต้ระบบการชำระเงินในปัจจุบัน และให้บริการทางการเงินให้แก่ลูกค้าซึ่งได้

ถือว่าการให้บริการทางการเงินของธนาคารพาณิชย์เป็นการให้บริการทางการเงินให้แก่ลูกค้าในระดับรายย่อย โดยมีรายละเอียดดังนี้

2.1 ATM หรือการให้บริการทางการเงินผ่านเครื่องฝากและถอนเงินอัตโนมัติ ไม่ว่า จะเป็นการฝากถอนหรือโอนเงินอัตโนมัติและปัจจุบันยังสามารถโอนเงินผ่านเครื่องATM ระหว่างธนาคารได้ทั่วประเทศ

2.2 การให้บริการโอนเงิน ณ จุดขาย(Electronic Fund Transfer at Point of Sale หรือ EFT-POS)

2.3 การให้บริการธนาคารทางโทรศัพท์ (Tele-Banking) บริการ TELEFAX

2.4 การให้บริการธนาคารในสำนักงานหรือบ้าน (Office Banking หรือ Home Banking)

2.5 การให้บริการโอนเงินตามข้อตกลงล่วงหน้า(Pre-authorized Transfer)

2.6 การให้บริการผ่านบัตรเครดิต (Credit Card) หรือบัตรเดบิต (Debit Card) ทั้งบัตรเดบิต หรือบัตรเครดิต ซึ่งบัตรดังกล่าวได้บรรจุคำสั่งในรูปคลื่นแม่เหล็กอยู่ภายใน หลังจากนั้นข้อมูลจะถูกอ่านและประมวลผลโดยอุปกรณ์ทางคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์ เช่น เครื่อง EDC, เครื่องฝากและถอนเงินอัตโนมัติ(ATM), เครื่องโอนเงิน ณ จุดขาย(POS) เป็นต้น ซึ่งการให้บริการดังกล่าวส่งผลให้สามารถเดบิตหรือเครดิตบัญชีตามคำสั่ง และสามารถชำระเงินตามคำสั่งดังกล่าวได้อย่างรวดเร็ว

2.7 การโอนเงินผ่านระบบออนไลน์ (On-line Banking Service) ของธนาคารพาณิชย์

2.8 การให้บริการชำระเงินในรูปแบบใหม่ที่เรียกว่า เงินอิเล็กทรอนิกส์ (E-money) เพื่ออำนวยความสะดวกในการชำระเงินจำนวนเล็กๆ น้อยๆ โดยมีลักษณะการให้บริการดังนี้

2.8.1 การชำระเงินผ่านไมโครชิพ (Smart Card) ไม่ว่าจะเป็น Visa card, Master card ซึ่งการทำงานต้องใช้ชำระเงินผ่านเครื่อง EDC ส่วน Mondex card และ Visa card นั้นเป็นบัตรประเภทที่สามารถขอเติมวงเงินในบัตรได้เรื่อยไป

2.8.2 การชำระเงินผ่านเครือข่ายอินเทอร์เน็ต ซึ่งผู้ใช้บริการสามารถดาวน์โหลดเงินอิเล็กทรอนิกส์จากธนาคารผ่านระบบอินเทอร์เน็ต หรือชำระค่าสินค้าหรือบริการต่างๆ จากการซื้อขายทางพาณิชย์อิเล็กทรอนิกส์ หรือโอนเงินอิเล็กทรอนิกส์ผ่าน

ระบบอินเทอร์เน็ตจากเครื่องคอมพิวเตอร์ของตนส่งผ่านระบบอิเล็กทรอนิกส์ไปยังบัญชีที่ต้องการโอนไปได้อย่างรวดเร็ว เปรียบได้ว่า ระบบอินเทอร์เน็ตเป็นเครือข่ายในการเชื่อมโยงข้อมูลในการทำธุรกรรมทางอิเล็กทรอนิกส์

2.8.3 บัตรพลาสติก (Plastic money) บัตรที่มีการบรรจุข้อมูลอันเป็นจำนวนเงินอยู่ในบัตร (prepaid card) โดยบัตรดังกล่าวจะต้องใช้กับอุปกรณ์อิเล็กทรอนิกส์เพื่อประมวลผลข้อมูลและโอนจ่ายเงินได้ในทันที เช่น บัตรโทรศัพท์ บัตร BTS บัตรพร้อมใช้ของโทรศัพท์เคลื่อนที่ เป็นต้น

2.9 คำสั่งในการทำธุรกรรมทางการเงินผ่านระบบสื่อสาร เช่น TELEFAX โทรศัพท์เคลื่อนที่ ซึ่งใช้เทคโนโลยีสารสนเทศในการส่งผ่านข้อมูลเพื่อการทำธุรกรรมทางอิเล็กทรอนิกส์และระบบดังกล่าวจะประมวลผลข้อมูลและส่งข้อมูลมายังธนาคารที่ผู้ส่งข้อมูลระบบ เพื่อดำเนินการทำธุรกรรมตามคำสั่งที่ส่งมานั้น

3. การโอนเงินทางอิเล็กทรอนิกส์ระหว่างประเทศผ่านระบบ SWIFT

SWIFT (Society for Worldwide Interbank Fund Transfer) เป็นเครือข่ายในสื่อสารระหว่างประเทศอิเล็กทรอนิกส์ผ่านระบบคอมพิวเตอร์ออนไลน์ ซึ่งอยู่ภายใต้กฎหมายเบลเยี่ยม โดยจัดตั้งขึ้นในรูปของ Co-Operation company เมื่อเดือนพฤษภาคม 2516 โดยมีสถาบันทางการเงินทั่วโลกเป็นสมาชิกและผู้ถือหุ้น และให้บริการในธุรกรรมทางการเงินต่าง ๆ ทั่วโลก เช่น การโอนเงิน การซื้อขายเงินตราระหว่างประเทศและการซื้อขายตราสาร (Letter of Credit) หรือหลักทรัพย์ประเภทต่างๆ ดังนั้นข้อมูลทางอิเล็กทรอนิกส์ที่ส่งผ่านระบบดังกล่าวจะต้องถูกจัดให้อยู่ในรูปแบบที่มีมาตรฐาน เพื่อป้องกันการผิดพลาด นอกจากนั้น การโอนเงินผ่านระบบ SWIFT นี้ยังมีกระบวนการในการรักษาความปลอดภัยอย่างเพียงพอ เพื่อให้การชำระเงินผ่านทางระบบ SWIFT สามารถเป็นไปได้อย่างเรียบร้อยรวดเร็ว และมีความปลอดภัยในโอนข้อมูลทางอิเล็กทรอนิกส์มากเพียงพอในการชำระเงินภายในประเทศและการชำระเงินระหว่างประเทศทั่วโลก

2.3.4 ประเภทของการโอนเงินทางอิเล็กทรอนิกส์

หากพิจารณาถึงลักษณะของการให้บริการโอนเงินทางอิเล็กทรอนิกส์นั้นสามารถแบ่งประเภทการโอนเงินทางอิเล็กทรอนิกส์ได้ตามวัตถุประสงค์แห่งการโอนเงินทางอิเล็กทรอนิกส์ได้ออกเป็น 2 ประเภท กล่าวคือ

1. การโอนเงินทางอิเล็กทรอนิกส์ที่มีวัตถุประสงค์ในการชำระเงิน

การโอนเงินทางอิเล็กทรอนิกส์ที่มีวัตถุประสงค์ในการชำระเงินกล่าวคือ การโอนเคลื่อนย้ายหรือส่งมอบเงินจากบุคคลหนึ่งไปยังอีกบุคคลหนึ่ง หรือจากที่หนึ่งไปยังอีกที่หนึ่ง โดยใช้คำสั่งหรือการป้อนข้อมูลผ่านเครื่องเทอร์มินัล เครื่องคอมพิวเตอร์ เครื่องประมวลผลข้อมูล อุปกรณ์หรือสื่อทางอิเล็กทรอนิกส์ ซึ่งเครื่องคอมพิวเตอร์ อุปกรณ์หรือสื่อทางอิเล็กทรอนิกส์ที่ได้รับคำสั่งจะทำหน้าที่แปลรหัสข้อมูลที่ได้รับ และหากเมื่ออ่านข้อมูลและรหัสที่ได้รับได้อย่างถูกต้องธนาคารพาณิชย์จะทำการอนุมัติให้โอน ส่งมอบ หรือเคลื่อนย้ายเงินเข้าหรือออกจากบัญชีได้ตามคำสั่งดังกล่าวเพื่อการชำระราคาค่าสินค้าหรือบริการ หรือเป็นการโอนเงินทางอิเล็กทรอนิกส์ที่เกิดขึ้นภายใต้ธุรกรรมประเภทต่างๆ ในทางแพ่งและพาณิชย์ หรือการโอนเงินทางอิเล็กทรอนิกส์ที่เกิดขึ้นภายใต้ธุรกรรมทางอิเล็กทรอนิกส์

2. การโอนเงินทางอิเล็กทรอนิกส์ที่ไม่มีวัตถุประสงค์ในการชำระเงิน

การโอนเงินทางอิเล็กทรอนิกส์ที่ไม่มีวัตถุประสงค์ในการชำระเงิน กล่าวคือ การโอน เคลื่อนย้ายหรือส่งมอบเงินจากบุคคลหนึ่งไปยังอีกบุคคลหนึ่ง หรือจากที่หนึ่งไปยังอีกที่หนึ่ง โดยใช้คำสั่งหรือการป้อนข้อมูลผ่านเครื่องเทอร์มินัล เครื่องคอมพิวเตอร์ เครื่องประมวลผลข้อมูล อุปกรณ์หรือสื่อทางอิเล็กทรอนิกส์ ซึ่งเครื่องคอมพิวเตอร์ อุปกรณ์หรือสื่อทางอิเล็กทรอนิกส์ที่ได้รับคำสั่งจะทำหน้าที่แปลรหัสข้อมูลที่ได้รับ และหากเมื่ออ่านข้อมูลและรหัสที่ได้รับได้อย่างถูกต้องธนาคารพาณิชย์จะทำการอนุมัติให้โอน ส่งมอบ หรือเคลื่อนย้ายเงินเข้าหรือออกจากบัญชีได้ตามคำสั่งดังกล่าว เพื่อวัตถุประสงค์ในการดำเนินการเปลี่ยนแปลงหรือเพื่อเคลื่อนไหวรายการทางบัญชีทางอิเล็กทรอนิกส์

2.4 อาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

ในสังคมปัจจุบันความก้าวหน้าทางด้านเทคโนโลยีคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ ได้เข้ามามีบทบาทต่อระบบการชำระเงินและระบบการเงินการธนาคารเป็นอย่างมาก ด้วยระบบคอมพิวเตอร์สามารถเก็บข้อมูล หรือส่งผ่านข้อมูลทางอิเล็กทรอนิกส์เพื่อดำเนินธุรกรรมต่างๆ ภายใต้ระบบการเงินการธนาคารให้เป็นไปได้อย่างสะดวกรวดเร็ว และครอบคลุมทั้งธุรกรรมภายในประเทศและต่างประเทศภายใต้การพัฒนาระบบคอมพิวเตอร์ในการติดต่อสื่อสารหรือการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์จากการติดต่อระหว่างระบบหรือเครือข่ายทางคอมพิวเตอร์ หรือระบบอิเล็กทรอนิกส์ จนในปัจจุบันได้มีการพัฒนาเข้าสู่การติดต่อสื่อสารหรือแลกเปลี่ยนข้อมูลระหว่างกันได้ทั่วโลก ด้วยความเจริญก้าวหน้าทางคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ดังกล่าว จึงทำให้มีผู้พยายามพัฒนากระบวนการในการโอนเงินทางอิเล็กทรอนิกส์ในลักษณะต่างๆ ในลักษณะเดียวกัน จึงทำให้เกิดการแสวงหาผลประโยชน์โดยทุจริตต่อกระบวนการโอนเงินทางอิเล็กทรอนิกส์ หรือการกระทำโดยใช้กระบวนการโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิดในลักษณะต่างๆ เพิ่มจำนวนมากขึ้นเป็นเงาตามตัวเช่นกัน ซึ่งสร้างความเสียหายต่อระบบการเงินการธนาคารและเสถียรภาพทางด้านการเงินการธนาคารของประเทศได้

2.4.1 ความหมายของคำว่า "อาชญากรรม"

หากกล่าวถึงคำว่า "อาชญากรรม" หมายถึง การกระทำใดๆ อันเป็นการฝ่าฝืน กฎระเบียบ ข้อบังคับ หรือกฎหมาย โดยมีเจตนาชั่วร้าย มีเจตนาอันมิชอบ หรือมีเจตนาทุจริต และก่อให้เกิดความเสียหายแก่บุคคลหรือสังคม หรือตามความหมายของพจนานุกรมฉบับราชบัณฑิตยสถาน ซึ่งได้ให้ความหมายของคำว่า "อาชญา" หมายถึง อำนาจ,โทษ ซึ่ง มักใช้สำหรับพระเจ้าแผ่นดินหรือเจ้านาย เช่น พระราชอาชญา: คดีที่เกี่ยวกับโทษหลวงเรียกว่า คดีอาชญา หรือความอาชญา คู่กับความแพ่ง ซึ่งไม่เกี่ยวด้วยโทษหลวงเช่นความมรดกเป็นต้น; ศาลที่ชำระความเกี่ยวกับโทษหลวงเรียกว่า ศาลอาชญา คู่กับศาลแพ่งซึ่งชำระความแพ่ง. คำอาชญานี้มักตัดใช้ว่า อาญา เป็นพื้น. และ "กรรม" หมายถึง การ, การกระทำ, การงาน, กิจ เช่น พลีกรรม; เป็นการดีก็ได้ การชั่วก็ได้ เช่น กุศลกรรม อกุศลกรรม ดังนั้นอาจสรุปความหมายของ "อาชญากรรม" ได้ว่า หมายถึง การกระทำการใดๆ อันเป็นการละเมิด หรือฝ่าฝืนต่อกฎหมายอันถือว่าเป็นความผิด และต้องได้รับโทษตามกฎหมาย

2.4.2. ประเภทของอาชญากรรมในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

หากพิจารณาถึงอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ สามารถแบ่งได้เป็น 2 ลักษณะ กล่าวคือ อาชญากรรมที่เป็นการกระทำต่อเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์ และอาชญากรรมที่เป็นการกระทำโดยอาศัยเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิดหรือแสวงหาผลประโยชน์โดยทุจริต

2.4.2.1 การฉ้อโกงทางคอมพิวเตอร์ หรืออาชญากรรมที่เป็นการกระทำต่อระบบการโอนเงินทางอิเล็กทรอนิกส์

อาชญากรรมที่เป็นการกระทำต่อระบบโอนเงินทางอิเล็กทรอนิกส์นั้นจะเห็นได้ว่าเป็นการกระทำอย่างหนึ่งอย่างใด ในการใช้ความรู้ความสามารถทางด้านเทคโนโลยีคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ หรือการกระทำการอย่างหนึ่งอย่างใดที่เป็นการกระทำต่อเครื่องหรือระบบอิเล็กทรอนิกส์ภายใต้กระบวนการโอนเงินทางอิเล็กทรอนิกส์ เพื่อแสวงหาผลประโยชน์โดยทุจริต ซึ่งการกระทำความผิดลักษณะใดๆ ในการใช้ความรู้ความสามารถทางด้านเทคโนโลยีคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ภายใต้กระบวนการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งจัดได้ว่าเป็นการฉ้อโกงทางคอมพิวเตอร์ หรือ "อาชญากรรมทางคอมพิวเตอร์" อย่างหนึ่ง

หากพิจารณาจากความหมายหรือคำนิยามของคำว่า "อาชญากรรมคอมพิวเตอร์" โดยนักวิชาการหรือสถาบันหรือองค์การต่างๆ ซึ่งได้ให้ความหมายของคำว่า "อาชญากรรมคอมพิวเตอร์" ไว้ดังนี้

ปาร์คเกอร์และซูซาน (Donn B.Parker and Susan H.nycum) ได้ให้คำนิยามไว้ว่า อาชญากรรมคอมพิวเตอร์เป็นการกระทำที่ผิดกฎหมาย โดยใช้เทคนิคหรือความรู้ทางด้านเทคโนโลยี สามารถแบ่งได้เป็น 4 ประการ

1. การใช้เป็นวัตถุหรือเหยื่อในการกระทำความผิด
2. การใช้เป็นสิ่งกระทำความผิดหรือสื่อในการกระทำความผิด
3. การใช้เป็นเครื่องมือในการกระทำความผิด

4. การใช้เป็นสัญลักษณ์ในการกระทำความผิด[7]

ทาเบอร์ (Taber) ได้ให้คำนิยามไว้ว่า อาชญากรรมคอมพิวเตอร์ที่แท้จริงต้องเป็นการกระทำที่มีข้อเท็จจริงเกิดขึ้นจากการกระทำของคอมพิวเตอร์โดยตรง หรือใช้เป็นเครื่องมือที่สำคัญในการกระทำความผิด (Taber,1980)[8]

โคเมอร์ (Comer) ให้คำนิยามไว้ว่าเป็นการทุจริตทางการเงินใดๆ ที่มีการใช้คอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ในการฉ้อโกงทางคอมพิวเตอร์ (Comer.1985)[9]

แมนเดล (Mandell) ได้ให้คำนิยามไว้ว่าอาชญากรรมคอมพิวเตอร์สามารถแบ่งการกระทำเป็น 2 ชนิดคือ

1. การใช้คอมพิวเตอร์เพื่อที่กระทำการหลอกลวง ลักขโมยหรือปิดบังซ่อนเร้น โดยเจตนาเพื่อที่จะให้ได้รับผลประโยชน์ทางการเงิน ทางธุรกิจ ทรัพย์สิน หรือผลประโยชน์ทางด้านการบริการและ
2. การดูกดามทางคอมพิวเตอร์ เช่น การจารกรรมคอมพิวเตอร์ ฮาร์ดแวร์ ซอฟต์แวร์ การก่อวินาศกรรม หรือการเรียกค่าไถ่(Mandell,1984)[10]

บิคไคย์ (Bequai) ให้คำนิยามไว้ว่าเป็นการกระทำใดๆ ที่ผิดกฎหมายโดยใช้ความรู้ ทางด้านเทคโนโลยีสารสนเทศอันเป็นสิ่งจำเป็นในการกระทำความผิด หรือใช้คอมพิวเตอร์เป็นประโยชน์ในการก่ออาชญากรรม รวมถึงการกระทำต่อสิ่งที่เก็บอยู่ในคอมพิวเตอร์ (Bequai,1978)[11]

ปาร์เกอร์ (Parker) ได้ให้คำนิยามไว้ว่าเป็นการใช้คอมพิวเตอร์กระทำการหลอกลวง ปิดบังซ่อนเร้น ใช้เล่ห์กล โดยมีวัตถุประสงค์ให้ได้รับทรัพย์สิน เงิน บริการ อำนาจทาง

---

[7] เลิศชาย สุธรรมพร.อาชญากรรมคอมพิวเตอร์: ศึกษากรณีความปลอดภัยของข้อมูล. (กรุงเทพมหานคร : วิทยานิพนธ์), 2541, หน้า 34-35.

[8] เรื่องเดียวกัน,หน้า 35.

[9] เรื่องเดียวกัน,หน้า 35.

[10] เรื่องเดียวกัน,หน้า 36.

[11] เรื่องเดียวกัน,หน้า 36.

การเมือง หรือประโยชน์ทางธุรกิจ และการคุกคามทางคอมพิวเตอร์ การก่อวินาศกรรม การเรียกค่าไถ่ รวมถึงการกระทำต่างๆ ที่ใช้คอมพิวเตอร์เป็นเครื่องมือหรือเป้าหมายในการกระทำความผิด (Parker,1983) [12]

องค์การเพื่อการพัฒนาและความร่วมมือทางเศรษฐกิจ หรือโออีซีดี (Organization for Economic Coorporation and Development : OECD) ได้ให้คำนิยามของคำว่า อาชญากรรมคอมพิวเตอร์ (Computer Crime) หรืออาชญากรรมเกี่ยวกับคอมพิวเตอร์ (Computer Related Crime) ไว้ว่า เป็นการกระทำใดๆ ที่ผิดกฎหมาย ผิดจริยธรรม หรือกระทำการโดยปราศจากอำนาจในการประมวลผลข้อมูลหรือส่งผ่านข้อมูล (OECD,1986)[13]

คณะกรรมาธิการตรวจสอบอำนาจท้องถิ่นของอังกฤษและเวลส์ (The Audit Commission for Local Authorities in England and Wales) ให้คำนิยามไว้ว่าเป็นการฉ้อโกงใดๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ โดยบุคคลนั้นเจตนาทุจริต เพื่อที่จะให้ได้รับผลประโยชน์ (The Audit Commission for Local Authorities in England and Wales,1987)[14]

คณะกรรมาธิการกฎหมายของอังกฤษ (The Law Commission UK) ได้ให้คำนิยามไว้ว่าเป็นการฉ้อโกงทางคอมพิวเตอร์ โดยกล่าวว่า " เป็นการกระทำของคอมพิวเตอร์ไม่ว่าด้วยวิธีใดๆ ก็ตามที่เป็นการทุจริตเพื่อให้ได้รับเงิน ทรัพย์สิน หรือประโยชน์ที่มีค่าอื่นๆ หรือทำให้เกิดความเสียหาย (The Law Commission UK,1988)[15]

กระทรวงยุติธรรมสหรัฐอเมริกา ได้ให้คำนิยามคำว่า "อาชญากรรมคอมพิวเตอร์" ไว้ว่าเป็นการกระทำที่ต้องอาศัยประสบการณ์ทางคอมพิวเตอร์ โดยทั่วไปอาชญากรรมประเภทนี้จะเกิดขึ้นภายในคอมพิวเตอร์ คำว่า "อาชญากรรมที่เกี่ยวกับคอมพิวเตอร์" เป็นคำที่กว้างกว่า หมายความถึงการกระทำความผิดทางอาญาที่อาศัยความรู้ทางด้านเทคโนโลยีสารสนเทศ เพื่อกระทำความผิด รวมทั้งการสืบสวนสอบสวนและฟ้องร้อง คำว่า "การใช้คอมพิวเตอร์

---

[12] เลิศชาย สุธรรมพร.อาชญากรรมคอมพิวเตอร์: ศึกษากรณีความปลอดภัยของข้อมูล. (กรุงเทพมหานคร : วิทยานิพนธ์), 2541,หน้า 36.

[13] เรื่องเดียวกัน,หน้า 35.

[14] เรื่องเดียวกัน,หน้า 35.

[15] เรื่องเดียวกัน,หน้า 35.

กระทำความผิด" เป็นการรวมความหมายที่กว้างคือการกระทำโดยเจตนาที่เป็นความผิดทางอาญา ซึ่งเป็นการกระทำโดยเจตนาใดๆ ที่อาศัยความรู้ทางด้านเทคโนโลยีสารสนเทศกระทำความผิดโดยบุคคลหนึ่งหรือมากกว่านั้นเพื่อที่จะให้เหยื่อได้รับความเสียหาย(The National Criminal Justice Information and Statistics Service,1989)[16]

ประเทศออสเตรีย ให้คำนิยามของคำว่า"อาชญากรรมคอมพิวเตอร์" ไว้ว่าเป็นการกระทำความผิดทางอาญาทุกชนิดที่อาศัยคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดหรือเป็นเป้าหมายในการกระทำความผิด (Schick,1993)[17]

ประเทศเยอรมัน โดยหน่วยงานของตำรวจสืบสวนสอบสวนได้ให้คำนิยามและจำแนกความหมายของคำว่า "อาชญากรรมคอมพิวเตอร์" เพื่อใช้ในการดำเนินคดีไว้ดังนี้ อาชญากรรมคอมพิวเตอร์ครอบคลุมถึงพฤติการณ์ที่เกี่ยวกับการประมวลผลข้อมูลทางอิเล็กทรอนิกส์ โดยเป็นวัตถุแห่งการกระทำความผิดหรือใช้เป็นสิ่งที่ช่วยในการกระทำความผิด (Mohrenschlager,1993)[18]

ประเทศญี่ปุ่นโดยสำนักงานตำรวจแห่งชาติได้ให้คำนิยามของคำว่า "อาชญากรรมคอมพิวเตอร์"ไว้ว่าเป็นอาชญากรรมซึ่งรวมถึงการกระทำโดยประมาทหรืออุบัติเหตุซึ่งขัดขวางการทำงานของระบบคอมพิวเตอร์ หรือใช้คอมพิวเตอร์ในทางที่ผิดกฎหมาย (Yamaguchi,1993) [19]

สำนักงานตำรวจแห่งชาติของประเทศไทยได้ให้ความหมายของคำว่า "อาชญากรรมทางคอมพิวเตอร์" ไว้ว่า

1. การกระทำใดๆ ก็ตามที่เกี่ยวกับการใช้คอมพิวเตอร์อันทำให้เหยื่อได้รับความเสียหาย และผู้กระทำได้รับผลประโยชน์ตอบแทน

---

[16] เลิศชาย สุธรรมพร.อาชญากรรมคอมพิวเตอร์: ศึกษากรณีความปลอดภัยของข้อมูล. (กรุงเทพมหานคร : วิทยานิพนธ์), 2541,หน้า 36.

[17] เรื่องเดียวกัน,หน้า 36.

[18] เรื่องเดียวกัน,หน้า 37.

[19] เรื่องเดียวกัน,หน้า 37.

2. การกระทำผิดกฎหมายใดๆ ซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือในการสืบสวนสอบสวนของเจ้าหน้าที่เพื่อนำตัวผู้กระทำความผิดมาดำเนินคดีก็ต้องใช้ความรู้ทางเทคโนโลยีคอมพิวเตอร์เช่นกัน[20]

จากที่กล่าวมาข้างต้นสามารถสรุปความหมายของคำว่า "อาชญากรรมคอมพิวเตอร์" ได้ว่าหมายถึง การกระทำใดๆ ซึ่งใช้ หรือใช้ความรู้ทางด้านคอมพิวเตอร์กระทำ หรือเป็นการกระทำโดยตรงต่อคอมพิวเตอร์ เครื่องเทอร์มินัล หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ไม่ว่าจะเป็นหน่วยประมวลผลข้อมูล หน่วยประมวลผลกลาง หน่วยรับข้อมูล หน่วยแสดงผล หน่วยความจำ หรือหน่วยใดๆ ในการทำงานของคอมพิวเตอร์เพื่อสั่งคำสั่งหรือชุดคำสั่งใด ๆ ส่งผ่านเพื่อให้คอมพิวเตอร์ทำงานและแสดงผลตามที่ต้องการอันเป็นการแสวงหาประโยชน์อย่างใดอย่างหนึ่งโดยมิชอบ เพื่อผลประโยชน์แก่ตนเองหรือบุคคลอื่นหรือกระทำเพื่อให้บุคคลอื่นได้รับความเสียหาย

หากพิจารณาเปรียบเทียบการโอนเงินทางอิเล็กทรอนิกส์ของระบบการเงินการธนาคารเป็นกระบวนการหนึ่งที่ได้นำระบบคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์ในการส่งคำสั่งข้อมูลทางอิเล็กทรอนิกส์แก่ระบบคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์ของระบบการเงินการธนาคารเพื่อให้เครื่องคอมพิวเตอร์ทำงาน และแสดงผลในการโอนเงินตามคำสั่งทางอิเล็กทรอนิกส์ดังกล่าวนั้น ดังนั้นอาชญากรรมที่เป็นการกระทำต่อเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์ถือได้ว่าเป็นอาชญากรรมทางคอมพิวเตอร์ โดยพิจารณาเปรียบเทียบความหมายของคำว่า "คอมพิวเตอร์" ซึ่งหมายถึง เครื่องอิเล็กทรอนิกส์ที่มีสมรรถนะในการประมวลผลของข้อมูลได้อย่างอัตโนมัติ โดยอาศัยคำสั่งหรือชุดคำสั่งที่เขียนขึ้นมาเป็น โปรแกรมกำหนดเงื่อนไขให้คอมพิวเตอร์ทำงานอย่างเป็นระบบด้วยความรวดเร็ว ที่ถูกต้องในการจดจำข้อมูลคิดคำนวณทางคณิตศาสตร์ การเคลื่อนย้ายข้อมูลและการพิมพ์ผลลัพธ์ออกมา ไม่ว่าจะมีการกำหนดในเรื่องของความจำ ข้อมูลหรือคำสั่งต่างๆ สลับซับซ้อนเพียงใดก็ตาม เครื่องคอมพิวเตอร์สามารถทำงานให้ได้ผลออกมาอย่างถูกต้อง ถ้าข้อมูลและคำสั่งที่ป้อนเข้าไปในเครื่องนั้นมีความถูกต้อง[21]

---

[20] สำนักงานตำรวจแห่งชาติ. สาระน่ารู้ : อาชญากรรมคอมพิวเตอร์. แหล่งที่มา : http://www.ecid.police.go.th.

[21] พีรพันธุ์ เปรมภูติ, เอกสารประกอบการสัมมนา เรื่อง สภาพปัญหาอาชญากรรมคอมพิวเตอร์, 2539.(เอกสารไม่ตีพิมพ์เผยแพร่)

คำนิยามตามพจนานุกรมอิเล็กทรอนิกส์ของนายรูดอล์ฟ เอฟ แกรฟ ได้ให้ความหมายของ "คอมพิวเตอร์" หมายถึง "เป็นอุปกรณ์ใดๆ ก็ได้ที่สามารถรับข้อมูลเข้าไปประมวลผลแล้วให้ผลลัพธ์อยู่ในรูปแบบที่เราต้องการ ชิ้นส่วนหลักที่ประกอบขึ้นเป็นคอมพิวเตอร์จะประกอบด้วย หน่วยความจำ หน่วยควบคุม หน่วยคำนวณผล และหน่วยรับข้อมูลและแสดงผล"[22] นอกจากนั้นคำนิยามตามพจนานุกรมอิเล็กทรอนิกส์ที่เรียบเรียงโดยนายวิทย์ เที่ยงบูรณธรรม ได้ให้ความหมายของคำว่า "Computer" หมายถึง เครื่องคำนวณ ผู้คำนวณ เครื่องคอมพิวเตอร์ คณิตกรณ์ เครื่องประมวลผลข้อมูล ซึ่งประกอบด้วยหน่วยประมวลผลกลาง หน่วยรับข้อมูล หน่วยแสดงผลและหน่วยความจำ เครื่องแรกประดิษฐ์ขึ้นโดยโรเจอร์ บิลลิงส์ลีย์ นักวิทยาศาสตร์ชาวอังกฤษเพื่อใช้เป็นเครื่องมือทรมานจอมเผด็จการฮิตเลอร์ เครื่องมือที่แก้ปัญหาได้ด้วยการรับข้อมูลเข้าไปและปฏิบัติการตามหัวข้อที่กำหนดให้กับข้อมูลนั้น และให้ผลตามที่กำหนดให้กับข้อมูลนั้นและให้ผลตามปฏิบัติการดังกล่าวออกมา มีอยู่หลายชนิดด้วยกัน เช่น เครื่องแอนาลอกคอมพิวเตอร์ (Analog Computer) เครื่องคำนวณ (Calcuator) และเครื่องดิจิตัลคอมพิวเตอร์ (Digital Computer)[23] ซึ่งหากพิจารณาเปรียบเทียบจากความหมายของคำว่า "อาชญากรรมคอมพิวเตอร์" และ "คอมพิวเตอร์" แล้วจึงกล่าวได้ว่าอาชญากรรมที่เป็นการกระทำโดยตรงต่อเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์จัดได้ว่าเป็นอาชญากรรมคอมพิวเตอร์อย่างหนึ่ง

2.4.2.1.1 ลักษณะของอาชญากรรมที่กระทำโดยตรงต่อเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์ซึ่งจัดว่าเป็นอาชญากรรมคอมพิวเตอร์

หากแบ่งอาชญากรรมคอมพิวเตอร์ที่เป็นการกระทำโดยตรงต่อเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์ตามลักษณะการทำงานของเครื่องคอมพิวเตอร์ หรือระบบอิเล็กทรอนิกส์นั้นสามารถแบ่งออกได้เป็น 5 ขั้นตอน ดังนี้

1. ขั้นตอนการนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์
2. ขั้นตอนการจัดโปรแกรมคอมพิวเตอร์
3. ขั้นตอนเกี่ยวกับการประมวลผลกลาง
4. ขั้นตอนการนำข้อมูลออกจากระบบคอมพิวเตอร์
5. ขั้นตอนการส่งผ่านข้อมูลคอมพิวเตอร์ไปยังจุดหมายปลายทาง

---

[22] ยืน ภู่วรรณ และคณะ. โปรแกรมคอมพิวเตอร์ภาษาเบสิค. (กรุงเทพมหานคร : เอเซียเพลส, 2527).

[23] วิทย์ เที่ยงบูรณธรรม. พจนานุกรมศัพท์คอมพิวเตอร์-อินเทอร์เนต.(พจนานุกรมอิเล็กทรอนิกส์,2545).

ด้วยเหตุนี้ อาชญากรรมคอมพิวเตอร์ที่เป็นการกระทำต่อเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์จึงเป็นการกระทำที่เกิดขึ้นโดยตรงต่อเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์ระหว่างขั้นตอนการทำงานของคอมพิวเตอร์ดังกล่าว ดังนี้

1. ขั้นตอนการนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์ในขั้นตอนการนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์นั้นเป็นการกระทำที่นำข้อมูลเข้าไปในเครื่องคอมพิวเตอร์ โดยข้อมูลดังกล่าวเป็นข้อมูลเท็จ หรือเป็นข้อมูลที่ไม่ถูกต้อง หรือมีการแก้ไขเปลี่ยนแปลงข้อมูล หรือการเข้าถึงเครื่องคอมพิวเตอร์โดยอาศัยข้อมูลที่มีรหัสผ่านหรือหมายเลขต่างๆ อัตโนมัติโดยปราศจากอำนาจ ซึ่งการกระทำเหล่านี้เรียกกันโดยทั่วไปว่า การโกงข้อมูล (Data Diddling) หรือ การโจมตีสลับ (Asynchronous Attacks) ซึ่งเป็นการอาศัยการทำงานสลับไปมาระหว่างคอมพิวเตอร์เป็นช่องว่างในการกระทำข้างต้น

2. ขั้นตอนการจัดโปรแกรมคอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์ในขั้นตอนการจัดโปรแกรมคอมพิวเตอร์นั้นเป็นการกระทำต่อโปรแกรมคอมพิวเตอร์ ซึ่งโปรแกรมคอมพิวเตอร์จัดเป็นศูนย์ควบคุมการทำงานของคอมพิวเตอร์อย่างสิ้นเชิง โดยโปรแกรมคอมพิวเตอร์จะเป็นหน่วยรับคำสั่งและจัดระบบหรือรูปแบบในการประมวลผลงานของคอมพิวเตอร์ตามโปรแกรรมคอมพิวเตอร์ ได้วางระบบไว้เรียบร้อยแล้วซึ่งอาชญากรรมคอมพิวเตอร์ในขั้นตอนนี้ได้ถูกเรียกตามรูปแบบที่แตกต่างกันดังนี้

2.1 ทร็อบดอร์ว (Trap Doors) เป็นการใช้ช่องว่างของโปรแกรมคอมพิวเตอร์เป็นช่องทางในการเข้าไปแก้ไขเปลี่ยนแปลงการทำงานของโปรแกรมคอมพิวเตอร์ โดยปกติโปรแกรมคอมพิวเตอร์ทั่วไปจะต้องมีการเว้นตำแหน่งช่องว่างไว้ในชุดคำสั่งหรือโปรแกรมดังกล่าวทุกครั้ง เพื่อใช้ในการเพิ่มคำสั่งหรือใช้ในการปรับปรุงแก้ไขโปรแกรมหรือเพิ่มความสามารถ หรือแก้ไขข้อผิดพลาดเล็กน้อยของโปรแกรมในภายหลัง ดังนั้นหากผู้เขียนโปรแกรมได้เปิดช่องว่างนั้นใหม่เพื่อแก้ไขโปรแกรมโดยทุจริต หรือมีบุคคลอื่นได้ค้นพบช่องว่างนั้นและอาศัยเป็นช่องทางในการทุจริตผ่านโปรแกรมคอมพิวเตอร์ดังกล่าว

2.2 โทรเจน ฮอร์ส (Trojan Horse) เป็นการแก้ไขเพิ่มเติม เปลี่ยนแปลงคำสั่งในโปรแกรมคอมพิวเตอร์ก่อนที่จะนำโปรแกรมไปใช้งาน โดยการซ่อนคำสั่งลับไว้ในโปรแกรมคอมพิวเตอร์ดังกล่าวให้ทำงานบางอย่างให้ พร้อม ๆ กับการทำงานโดยปกติของโปรแกรมคอมพิวเตอร์นั้นๆ และในบางโปรแกรมผู้ทุจริตสามารถเขียนคำสั่งให้โปรแกรมคอมพิวเตอร์นั้นทำลายคำสั่งดังกล่าวภายหลังจากที่ปฏิบัติภาระกิจเสร็จสิ้นแล้ว เช่นนี้ทำให้ไม่สามารถค้นพบหลักฐานในการกระทำความผิดจากโปรแกรมคอมพิวเตอร์ดังกล่าวได้

2.3 โลจิก บอมส์ (Logic Boms) เป็นการใช้คำสั่งลับในการป้อนคำสั่งแก่คอมพิวเตอร์ให้ทำงานตามที่ต้องการ โดยไม่ว่าคอมพิวเตอร์จะอยู่ในสภาวะใด ๆ หรือวันเวลาใด ๆ โปรแกรมลับนี้จะแอบซ่อนเข้าไปในโปรแกรมการทำงานของคอมพิวเตอร์ให้ทำงานให้เป็นระยะๆ หรือตามวันเวลาที่กำหนดไว้ และเมื่อถึงวันและเวลาที่กำหนดในระยะเวลาหนึ่งเวลาใด คำสั่งนี้จะกลายเป็นระเบิดการทำงานของคอมพิวเตอร์เมื่อเสร็จสิ้นภาระกิจ คำสั่งลับนี้จะทำงานในการทำลายข้อมูลที่เกี่ยวข้องกับโปรแกรมคอมพิวเตอร์นั้นๆ ทั้งหมด

2.4 ซุปเปอร์ แซปปิ้ง (Super Zapping) เป็นโปรแกรมคอมพิวเตอร์สำรองเพื่อใช้ในการไขรหัสต่างๆ หรือเป็นเครื่องมือพิเศษของระบบต่างๆ หรืออำนวยความสะดวกในการเข้าไปใช้โปรแกรมคอมพิวเตอร์ตัวจริง ซึ่งโปรแกรม Super Zapping นี้จะใช้ในกรณีฉุกเฉินที่ไม่อาจใช้โปรแกรมคอมพิวเตอร์ตัวจริงได้ จึงเปรียบเสมือนกุญแจสำคัญในการเปิดใช้โปรแกรมคอมพิวเตอร์ตัวจริง และเปรียบเสมือนเป็นดาบสองคมหากโปรแกรมดังกล่าวถูกใช้โดยผู้ทุจริต

2.5 ซาลามิ เทคนิค (Salami Techniques) เป็นโปรแกรมคอมพิวเตอร์ที่เขียนขึ้นเพื่อสั่งให้คอมพิวเตอร์ทำงานโดยปัดเศษสตางค์ในบัญชีของบุคคลอื่น ๆ ทั้งหมดในระบบนั้นโอนมาเข้าในบัญชีหนึ่งบัญชีใดตามที่ต้องการ

2.6 ไวรัส (Virus) เป็นโปรแกรมหรือคำสั่งที่เขียนขึ้นเพื่อทำลายข้อมูลในระบบนั้นทั้งหมด ซึ่งโปรแกรมไวรัสนี้จะทำลายข้อมูลส่วนใดของระบบนั้น ๆ บ้างย่อมเป็นไปตามที่ผู้เขียนโปรแกรมไวรัสนั้นได้กำหนดไว้

3. ขั้นตอนการประมวลผลกลาง

อาชญากรรมคอมพิวเตอร์ที่เกี่ยวกับการประมวลผลกลางนั้นมักเป็นการกระทำที่กระทำต่อหน่วยความจำ หรือหน่วยแปลคำสั่งหรือหน่วยปฏิบัติงานของคอมพิวเตอร์ ซึ่งอาจเป็นการสกัดกั้นไม่ให้ข้อมูลสามารถแปลคำสั่งได้ หรือการเปลี่ยนแปลงข้อมูลในหน่วยความจำหรือข้อมูลหลักให้เปลี่ยนแปลงไป ซึ่งการกระทำในรูปแบบนี้อาจเป็นการกระทำทั้งการทำลายหรือการแก้ไขเปลี่ยนแปลงข้อมูลก็ได้

4. ขั้นตอนเกี่ยวกับการนำข้อมูลออก

อาชญากรรมคอมพิวเตอร์ที่เกี่ยวกับการนำข้อมูลออกเป็นการกระทำต่อข้อมูลข่าวสารที่ได้รับจากหน่วยประมวลผลกลาง หรือข้อมูลข่าวสารหลังจากมีการแปลคำสั่งหรือข้อมูลข่าวสารที่ได้ผลิตออกมาจากระบบคอมพิวเตอร์ ซึ่งเรียกกันโดยทั่วไปว่า "การลักขโมยข้อมูล" หรือการเคลื่อนย้ายข้อมูลที่ได้จากระบบคอมพิวเตอร์หรือการแอบซ่อนข้อมูลที่ต้องการให้นำออกมาพร้อมกับข้อมูลปกติที่ผลิตตามคำสั่งโดยทั่วไป

5. ขั้นตอนการสื่อผ่านข้อมูลไปยังจุดหมายปลายทาง

อาชญากรรมคอมพิวเตอร์ในขั้นตอนของการส่งผ่านข้อมูลหรือคำสั่งใด ๆ ไปยังจุดหมายปลายทาง หรือการกระทำต่อการสื่อสารข้อมูลผ่านคอมพิวเตอร์นั้นๆ หรือ การกระทำต่อการเชื่อมต่อหรือการส่งผ่านข้อมูลระหว่างคอมพิวเตอร์กับสถานีรับส่งทั้งหลาย เช่น การดักข้อมูลระหว่างการส่งข้อมูลผ่านทางอิเล็กทรอนิกส์ เป็นต้น

ด้วยเหตุนี้ หากบุคคลใดบุคคลหนึ่งที่จะแสวงหาหรือใช้ประโยชน์จากระบบการเงินการธนาคารดังกล่าวโดยใช้ความรู้ความสามารถ และมีความเชี่ยวชาญเกี่ยวกับระบบคอมพิวเตอร์และระบบอิเล็กทรอนิกส์นี้โดยเฉพาะ และหากบุคคลดังกล่าวได้กระทำการใดๆ โดยมีเจตนามิชอบหรือมีเจตนาทุจริตเพื่อเจาะผ่านระบบอิเล็กทรอนิกส์ของระบบการเงินการธนาคารในการโอนเงินหรือการทำธุรกรรมใดๆ ผ่านทางอิเล็กทรอนิกส์ของระบบการเงินการธนาคาร เพื่อให้เงินดังกล่าวโอนเข้ามายังบัญชีที่ตนต้องการ หรือเพื่อให้ได้เงินดังกล่าวด้วยวิธีใด ๆ ตามที่ต้องการหรือตามคำสั่งที่กำหนดผ่านระบบอิเล็กทรอนิกส์ การกระทำความผิดในการโอนเงินทาง

อิเล็กทรอนิกส์ดังกล่าวจึงจัดเป็นอาชญากรรมคอมพิวเตอร์ที่มีความซับซ้อน และการป้องกันปราบปรามได้ยากมากขึ้นในปัจจุบัน

2.4.2.1.2 รูปแบบของอาชญากรรมกระทำต่อเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์

2.4.2.1.2.1 การโอนเงินโดยการปลอมแปลงข้อมูลทางอิเล็กทรอนิกส์เพื่อส่งคำสั่งโอนเงินทางอิเล็กทรอนิกส์

การกระทำความผิดในลักษณะนี้ เป็นการกระทำต่อระบบอิเล็กทรอนิกส์ของระบบการเงินการธนาคาร ไม่ว่าจะเป็นการกระทำการปลอมแปลงข้อมูลอิเล็กทรอนิกส์ของบัตรที่มีแถบแม่เหล็ก หรือรหัสผ่านของบัตรที่มีแถบแม่เหล็ก หรือรหัสผ่านของพนักงานธนาคาร ไม่ว่าจะเป็นการปลอมแปลงข้อมูลในการส่งคำสั่งโอนเงินทางอิเล็กทรอนิกส์ในธุรกรรมทางแพ่งและพาณิชย์ต่างๆ เช่น การสั่งซื้อขายสินค้าในระบบอินเทอร์เน็ต หรือที่เรียกกันว่า "ธุรกรรมอิเล็กทรอนิกส์" ประเภทต่างๆ หรือการปลอมแปลงข้อมูลอิเล็กทรอนิกส์เพื่อการส่งคำสั่งโอนเงินผ่านระบบธนาคารทางอินเทอร์เน็ต เพื่อการดำเนินธุรกรรมทางด้านการเงินการธนาคาร หรือ E-banking เป็นต้น

2.4.2.1.2.2 การโอนเงินโดยการทำลายข้อมูลทางอิเล็กทรอนิกส์ของระบบโอนเงินทางอิเล็กทรอนิกส์ที่ใช้หรือเกี่ยวข้องหรือเป็นข้อมูลในการตรวจสอบความถูกต้องของการโอนเงินทางอิเล็กทรอนิกส์ภายใต้ระบบการเงินการธนาคาร

การโอนเงินโดยการทำลายข้อมูลทางอิเล็กทรอนิกส์ของระบบโอนเงินทางอิเล็กทรอนิกส์นั้นจะต้องเป็นข้อมูลที่ใช้หรือเกี่ยวข้องหรือเป็นข้อมูลในการตรวจสอบความถูกต้องของการโอนเงินทางอิเล็กทรอนิกส์นั้น และการทำลายข้อมูลนั้นมีวัตถุประสงค์ เพื่อให้สามารถส่งคำสั่งในการโอนเงินเพื่อแสวงหาประโยชน์โดยทุจริตผ่านระบบการโอนเงินทางอิเล็กทรอนิกส์ได้ตามต้องการ

2.4.2.1.2.3 การโอนเงินโดยการเจาะหรือการแทรกแซงต่อระบบโอนเงินอิเล็กทรอนิกส์ รหัสผ่าน หรือข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์

การโอนเงินโดยการเจาะหรือการแทรกแซงต่อระบบโอนเงินทางอิเล็กทรอนิกส์ รหัสผ่าน หรือข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์นั้น ซึ่งกรณีนี้ต้องเป็นการกระทำต่อโปรแกรม ระบบ หรือรหัสผ่านที่เกี่ยวข้องกับระบบโอนเงินทางอิเล็กทรอนิกส์ หรือเพื่อให้ได้ข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าว

2.4.2.1.2.4 การโอนเงินโดยการแจ้งข้อมูลอันเป็นเท็จหรือการแจ้งข้อมูลที่ไม่ตรงกับความจริง ซึ่งอาจเป็นการกระทำที่พนักงานเจ้าหน้าที่ธนาคารอาจมีส่วนร่วมรู้เห็นด้วยหรือไม่ก็ได้ เพื่อการโอนเงินทางอิเล็กทรอนิกส์ในการแสวงหาประโยชน์จากการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าวโดยทุจริต

การโอนเงินหรือการกระทำอย่างหนึ่งอย่างใด โดยแจ้งข้อมูลอิเล็กทรอนิกส์ที่เป็นเท็จหรือไม่ตรงตามความจริงเพื่อให้การส่งคำสั่งโอนเงินทางอิเล็กทรอนิกส์เพื่อแสวงหาผลประโยชน์โดยทุจริต ไม่ว่าจะเป็นการโอนเงินผิดบัญชี หรือโอนเงินมากกว่าคำสั่งของผู้สั่งโอน ซึ่งการแสวงหาประโยชน์โดยทุจริตจากการกระทำดังกล่าวจากการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งการกระทำความผิดลักษณะนี้จะต้องมีการปลอมแปลงเอกสารหรือข้อมูลทางอิเล็กทรอนิกส์ร่วมด้วย เช่นการยักยอกเงินในบัญชีธนาคารของประชาชนหรือลูกค้า โดยพนักงานเจ้าหน้าที่ หรือการให้ข้อมูลที่ผิดไปจากความเป็นจริงในการสั่งโอนเงินจากบัญชีของคนอื่นเพื่อโอนเข้าสู่บัญชีของตน เป็นต้น

2.4.2.2 อาชญากรรมที่เป็นการกระทำโดยอาศัยเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิดหรือแสวงหาผลประโยชน์โดยทุจริต

ระบบโอนเงินทางอิเล็กทรอนิกส์เป็นระบบที่ใช้การอำนวยความสะดวกในการเคลื่อนย้ายเงินจากที่หนึ่งไปยังอีกที่หนึ่งได้อย่างสะดวกและรวดเร็ว ผ่านระบบ

อิเล็กทรอนิกส์ซึ่งเป็นที่นิยมอย่างแพร่หลายปัจจุบัน ซึ่งหากมองในอีกแง่หนึ่งแล้ว ระบบดังกล่าวได้ถูกนักคอมพิวเตอร์ที่มีความชำนาญทางด้านธุรกิจ และระบบการโอนเงินทางอิเล็กทรอนิกส์ซึ่งเห็นประโยชน์หรือกำไรที่สามารถเกิดขึ้นได้จากการโอนเงินทางอิเล็กทรอนิกส์ รวมไปถึงอาชญากรหรือองค์กรอาชญากรรมระหว่างประเทศนั้นได้มองเห็นประโยชน์จากการใช้กระบวนการโอนเงินทางอิเล็กทรอนิกส์เพื่อปกปิด อำพรางการเคลื่อนย้ายเงินเพื่อแสวงหาประโยชน์ในลักษณะหนึ่งลักษณะใดโดยผิดกฎหมาย ซึ่งลักษณะของอาชญากรรมที่เป็นการกระทำโดยอาศัยเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิดหรือแสวงหาผลประโยชน์โดยทุจริตที่เกิดขึ้นในปัจจุบัน มีดังต่อไปนี้

2.4.2.2.1 การลักลอบโอนเงินออกนอกประเทศ เพื่อแสวงหาประโยชน์เชิงธุรกิจซึ่งทำให้เงินไหลเวียนของประเทศออกนอกประเทศเป็นจำนวนมาก ซึ่งจะส่งผลทำให้เป็นการทำลายระบบการเงินการธนาคารและระบบเศรษฐกิจของประเทศไทย หรือการค้าอัตราแลกเปลี่ยน (FOREX)

การโอนเงินออกนอกประเทศโดยปกติ จะต้องมีการขออนุญาตจากธนาคารแห่งประเทศไทยจึงถือว่าเป็นการโอนเงินอย่างถูกต้อง กล่าวคือเป็นการรายงานถึงจุดประสงค์ในการโอนเงินออกนอก แต่การโอนเงินออกนอกประเทศเป็นจำนวนมาก โดยปกติจะไม่ได้รับอนุญาตจากธนาคารแห่งประเทศไทย ด้วยสาเหตุว่าการโอนเงินออกนอกประเทศเป็นจำนวนมากๆ จะส่งผลทำให้ปริมาณเงินภายในประเทศไหลออกนอก ซึ่งเช่นนี้หากมีการโอนเงินไหลออกนอกประเทศมากจนทำให้เงินไหลออกนอกระบบมากเกินไป ย่อมจะเป็นการทำลายเสถียรภาพของระบบการเงินการธนาคาร และย่อมส่งผลต่อระบบเศรษฐกิจ มหภาคของประเทศได้ ดังนั้นการโอนเงินออกนอกประเทศเป็นจำนวนมากจึงต้องทำการลักลอบโอนเงินไปยังต่างประเทศ

<u>วิธีการลักลอบโอนเงินออกนอกประเทศ</u>

กลุ่มบุคคลที่ประสงค์ต้องการโอนเงินไปต่างประเทศ ต้องการซื้อเงินตราต่างประเทศ (ดอลล่าร์สหรัฐ) แล้วทำการโอนเงินดังกล่าวออกนอกประเทศ แต่บุคคลอาจไม่สามารถที่จะดำเนินการด้วยตนเองได้ เนื่องจากกระทรวงการคลัง ได้ออกระเบียบ ขั้นตอนการดำเนินการประกอบกับพระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485 ได้กำหนดวิธีการ ขั้นตอนการดำเนินการ และหน้าที่รับผิดชอบของผู้ขายและผู้ขอซื้อเงินตราต่างประเทศไว้ทำให้บุคคลเหล่านั้นไม่สามารถขอซื้อเงินตราต่างประเทศเพื่อส่งออกนอกประเทศไทยได้ ด้วยเหตุดังกล่าวจึงได้มี

การจ้างให้บุคคลอื่นกระทำการดังกล่าวแทน เพื่อความสะดวกและทำให้การตรวจสอบทางเดินเงินได้ยากขึ้น โดยทั่วไปการขอซื้อเงินตราต่างประเทศจากธนาคาร หรือสถาบันการเงิน หรือที่เรียกว่า ตัวแทนรับอนุญาต จะใช้เหตุผลในการขอซื้อเงินตราต่างประเทศดังกล่าว2 ประการคือ

1. การขอซื้อเงินตราต่างประเทศเพื่อนำไปชำระหนี้เงินกู้จากต่างประเทศ

กรณีนี้ ต้องใช้เอกสารหลักฐานประกอบการขอซื้อ เช่น

1.1 หลักฐานการกู้ยืม เช่น สัญญากู้

1.2 หลักฐานการนำเงินเข้า (CREDIT ADVICE) ซึ่งออกโดยธนาคารเพื่อเป็นหลักฐานว่ามีการนำเงินจากต่างประเทศเข้ามาในประเทศ

ในกรณีนี้ เมื่อมีการขอซื้อเงินตราต่างประเทศแล้วและเมื่อต้องการให้สถาบันการเงินโอนเงินออกนอกประเทศจะต้องแจ้งวัตถุประสงค์ในการส่งเงินออกประเทศด้วย ซึ่งกรณีนี้ต้องรายงานในแบบรายงาน ธ.ต. 4 ที่ธนาคารแห่งประเทศไทยกำหนด โดยผู้ขอซื้อเงินตราต่างประเทศดังกล่าวต้องเป็นผู้กรอกรายละเอียดและลงนามในเอกสารดังกล่าวด้วย

2. เป็นการขอซื้อเงินตราต่างประเทศเพื่อชำระค่าสินค้าที่สั่งซื้อมาจากต่างประเทศ

กรณีนี้ ต้องใช้เอกสารหลักฐานประกอบการขอซื้อ เช่น

2.1 ใบขนสินค้า (B/L)

2.2 .ใบกำกับสินค้า (INVOICE)

แต่ในการดำเนินการของผู้รับจ้างโอนโดยกลุ่มบุคคลที่มารับจ้างในการโอนเงินนั้นอาจเคยหรือมี หรือมีความชำนาญในการทำธุรกิจส่งออกนำเข้าสินค้าจากต่างประเทศและเห็นช่องทางในการดำเนินการดังกล่าว ก็จะอาศัยช่องว่างดังกล่าวในการดำเนินการดังกล่าวโดยการปลอมเอกสารหลักฐานประกอบคำขอซื้อ และนำหลักฐานเดิมมาเวียนใช้ซ้ำ ทำให้สามารถขอซื้อและสั่งให้สถาบันการเงินโอนเงินออกนอกประเทศได้มากกว่าความเป็นจริง เนื่องจากสถาบันการเงินไม่คิดว่าจะมีการขอซื้อเงินตราต่างประเทศเพื่อชำระหนี้มากกว่าที่ตนเองเป็นหนี้อยู่ ในส่วนของการชำระค่าสินค้าก็ไม่มีผู้ใดคิดว่าจะมีการส่งเงินไปชำระค่าสินค้ามากกว่าที่ตนเองสั่งซื้อมา ดังนั้นการตรวจสอบของสถาบันการเงินที่เป็นผู้รับผิดชอบจึงอาจไม่ได้รอบคอบรัดกุมในการตรวจมากนั้น หรืออาจมีพนักงานของสถาบันการเงินคอยให้ความสะดวกจึงทำให้สามารถดำเนินการดังกล่าวรวดเร็วขึ้น

ปัจจัยที่ส่งผลทำให้สามารถขอซื้อและโอนเงินตราต่างประเทศออกนอกประเทศได้ กล่าวคือ

1. ในการสั่งซื้อเงินตราต่างประเทศและทำให้การโอนเงินออกนอกประเทศนั้นต้องทำด้วยความรวดเร็ว เนื่องจากอัตราแลกเปลี่ยนเงินเปลี่ยนแปลงตลอดเวลา หากทำรายการช้าสถาบันการเงินอาจเกิดความเสียหายจากอัตราแลกเปลี่ยนเงินได้

2. เนื่องจากต้องมีเวลาในการดำเนินการจำกัด ดังนั้นจึงส่งผลทำให้ไม่สามารถตรวจสอบเอกสารที่นำมาประกอบการขอซื้อได้อย่าง

3. เอกสารบางอย่างต้องตรงสอบจากหน่วยราชการที่เกี่ยวข้อง และข้อมูลของหน่วยราชการบางหน่วยเป็นความลับทำให้เสียเวลานานในการตรวจสอบ แต่ภายใต้เวลาที่จำกัดในการดำเนินการทำให้ไม่สามารถตรวจสอบได้

ดังนั้นการขอซื้อเงินตราต่างประเทศเพื่อโอนไปยังต่างประเทศเพื่อชำระหนี้เงินกู้ หรือชำระหนี้ค่าสินค้า ซึ่งใช้หลักฐานเท็จหรือปลอม หรือการใช้หลักฐานฉบับเดิมแสดงซ้ำหรือเวียนหลักฐานฉบับเดิมนั้น กรณีนี้สามารถลักลอบโอนเงินออกนอกประเทศได้เป็นจำนวนมากและง่ายสะดวกที่สุด และเป็นช่องทางในการโอนเงินออกนอกประเทศได้เป็นจำนวนมากหรือโอนได้มากกว่าจำนวนหนี้ตามหลักฐานที่แสดงอยู่ดังกล่าวโดยการขอโอนหลายๆ ครั้ง ด้วยหลักปฏิบัติของธนาคารจะมองว่า "ลูกหนี้จะไม่ชำระหนี้เกินกว่าจำนวนหนี้ที่มีอยู่" สาเหตุนี้ทำให้กระบวนการนี้สามารถลักลอบโอนเงินออกนอกประเทศเพื่อแสวงหาผลประโยชน์ในเชิงธุรกิจได้เป็นจำนวนมาก

หากพิจารณาถึง การลักลอบโอนเงินออกนอกประเทศดังกล่าวมักมีวัตถุประสงค์ในการค้ากำไรจากอัตราแลกเปลี่ยนเงินระหว่างประเทศ ซึ่ง รศ.ดร.สมภพ มานะรังสรรค์ นักวิชาการทางด้านเศรษฐศาสตร์ ได้ให้คำนิยามการทำธุรกิจแบบนี้ว่าเป็น "เศรษฐกิจแบบกาสิโน" โดยกล่าวว่า "ระบบเศรษฐกิจโลกทุกวันนี้เป็นยุคที่เรียกว่า เศรษฐกิจแบบกาสิโน ไม่ได้เป็นระบบเศรษฐกิจผลิตสินค้าเพื่อเอาไปขายเป็นเงินอย่างเมื่อก่อน จุดสุดท้ายของทุกธุรกิจที่ทำไป.. เพื่อหวังเงินกันทั้งนั้น ไหนๆ ก็ทำเพื่อเงินกันอยู่แล้ว เรื่องอะไรจะมาเสียเวลาผลิตสินค้า เอาเงินไปซื้อเงิน ขายเงิน ฟันกำไร.. ได้เงินเร็วกว่าเยอะ"[24] เช่นนี้ เป็นระบบที่มีการนำเงินไปซื้อเงิน ขายเงินเพื่อแสวงหากำไรจากความแตกต่างของอัตราแลกเปลี่ยนเงินระหว่างประเทศ หรือที่เรียกทั่วไปว่า "การค้าค่าเงิน" เพราะค่าเงินทุกสกุลในตลาดโลกมีอ่อนมีแข็ง มีอัตราแลกเปลี่ยนที่ไม่คงที่และมีส่วนต่างของค่าเงินให้หากำไรได้ตลอดเวลา ยกตัวอย่างเช่น กรณีเมื่อค่าเงินบาทแข็งก็

---

[24] รศ.ดร.สมภพ มานะรังสรรค์,สกู๊ปหน้า 1. หนังสือพิมพ์ไทยรัฐ (9 เมษายน 2545): 17.

แลกเป็นเงินดอลลาร์เก็บ แต่เมื่อเงินบาทอ่อนตัวก็เทเงินดอลลาร์ดังกล่าวออกขายทำกำไร การลักลอบโอนเงินออกนอกประเทศเพื่อการซื้อขายหุ้นระยะสั้น เพื่อการหากำไรจากการซื้อขายหรือส่วนต่างของราคาหุ้นในตลาดต่างประเทศ

2.4.2.2.2 การโอนเงินทางอิเล็กทรอนิกส์เพื่อปกปิด หรืออำพรางเงินจำนวนดังกล่าว โดยมีวัตถุประสงค์เพื่อการฟอกเงินหรือหลบเลี่ยงฐานภาษี

การโอนเงินทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นการโอนเงินทางอิเล็กทรอนิกส์ภายในประเทศหรือการโอนเงินออกนอกประเทศ โดยไม่มีวัตถุประสงค์หวังค้ากำไรจากการซื้อขายเงินตราต่างประเทศ แต่เป็นการโอนหรือเคลื่อนย้ายเงินดังกล่าวเพื่อปกปิดหรืออำพรางที่มาของเงินนั้น ซึ่งอาจมีวัตถุประสงค์ในการปกปิด หรืออำพรางที่มาของเงินที่ได้มาจากการกระทำความผิด หรือการโอนเงินจำนวนดังกล่าวเพื่อการเปลี่ยนแปลงสถานะของเงินจำนวนดังกล่าวจากเงินที่ได้มาจากการกระทำความผิดเป็นเงินที่ได้มาจากระบบการเงินการธนาคารอย่างถูกต้อง หรือฟอกเงินดังกล่าวให้เป็นเงินบริสุทธิ์ หรือหลบเลี่ยงภาษีจากการดำเนินธุรกิจของตนที่ต้องจ่ายให้แก่รัฐ และเงินดังกล่าวก็สามารถโอนกลับเข้ามาเพื่อดำเนินธุรกรรมอื่นใดของตนได้ต่อไป ซึ่งการโอนเงินทางอิเล็กทรอนิกส์อาจถูกใช้เป็นเครื่องมือในการฟอกเงินทั้งสิ้น

หากกล่าวถึงสถานที่ที่มักใช้ในการปกปิด อำพรางโดยการโอนเงินที่มีปรากฏอยู่ในปัจจุบัน ได้แก่ แหล่งที่มีการ โอนเงินเสรีที่ไม่มีการเก็บภาษีและรักษารายชื่อผู้ที่เกี่ยวข้องในการโอนเงินดังกล่าวไว้เป็นความลับ ซึ่งที่เป็นที่รู้จักอย่างมากในปัจจุบัน เช่น เกาะบริติช เวอร์จิ้น หรือที่เรียกกันว่า สวรรค์แห่งการฟอกเงิน ซึ่งระบบดังกล่าวไม่มีการเก็บภาษีในการโอนเงินทางอิเล็กทรอนิกส์ และไม่มีการเปิดเผยข้อมูลลูกค้า ซึ่งข้อมูลของลูกค้าจะถูกเก็บรักษาเป็นความลับไว้เป็นอย่างดีทำให้สถานที่ดังกล่าวกลายเป็นสวรรค์ของนักฟอกเงิน หรือปกปิดอำพรางเงินได้เป็นอย่างดี

2.4.2.2.3 การดำเนินกิจการบริษัทค้าอัตราแลกเปลี่ยนเงินตราต่างประเทศ (FOREX) โดยการระดมทุนของประชาชนผ่านการโอนเงินทางอิเล็กทรอนิกส์

การดำเนินกิจการบริษัทค้าอัตราแลกเปลี่ยนเงินตราต่างประเทศนี้จะดำเนินธุรกรรมปริวรรตเงินตราโดยอาศัยกำไรจากค่าต่อรองของสกุลเงินต่าง ๆ ซึ่งกระทรวง

การคลังไม่เคยออกใบอนุญาตสำหรับการทำธุรกรรมปริวรรตเงินตราให้แก่บริษัทเอกชนรายใด ดังนั้นบริษัทเหล่านี้จึงเป็นบริษัทลอยที่ทำการระดมทุนจากประชาชนที่สนใจค้าอัตราแลกเปลี่ยนสกุลเงินต่างๆ โดยประชาชนที่สนใจนั้นจะต้องโอนเงินให้แก่บริษัททำให้บริษัทดังกล่าวมีเงินโอนเข้าสู่บัญชีของบริษัทอย่างต่อเนื่อง[25]

บริษัทดังกล่าวจะคิดค่าคอมมิชชั่นในการค้าอัตราแลกเปลี่ยนนี้ทันที นับแต่เงินโอนเข้าสู่บัญชีของบริษัท แต่จะเสนอข้อแลกเปลี่ยนจากการค้าเงินตราต่างประเทศซึ่งคุ้มค้าให้แก่คนที่โอนเงินเข้ามานั้น แต่ข้อเสนอนั้นจะเป็นเพียงการบอกเล่าจากนักเทรดเดอร์ หรือมือเศรษฐกิจ ซึ่งได้แก่นักเก็งกำไรของบริษัทนั้น โดยในช่วงแรกการค้าอัตราแลกเปลี่ยนจะทำกำไรให้แก่ลูกค้าได้เป็นจำนวนมาก ซึ่งบริษัทจะเรียกเก็บค่าคอมมิชชั่นจากเงินในส่วนนี้อีกทางหนึ่ง หลังจากนั้นเมื่อดำเนินการค้าอัตราแลกเปลี่ยนดังกล่าวไปในระยะหนึ่ง จะมีพลิกผันของสถานการณ์การค้าเงินทำให้เงินจำนวนดังกล่าวของลูกค้าหายไปในทันที ซึ่งกรณีนี้นักเทรดเดอร์จะแจ้งว่าถือเป็นเรื่องปกติ และลูกค้าจะต้องเติมเงินเข้ามาให้แก่บริษัทเพื่อลงทุนใหม่ โดยลูกค้าจะมองว่าหากไม่โอนเงินให้อีกจะต้องเสียเงินก้อนแรกที่ลงทุนไปทั้งหมด จึงทำให้เป็นสาเหตุสำคัญในการตัดสินใจโอนเงินเข้ามาให้แก่บริษัทนี้อีก และการดำเนินกิจการจะเป็นไปในลักษณะเดิม หรือบางครั้งบริษัทอาจทำการฉ้อโกง โดยหลอกลวงว่าทำการซื้อขายอัตราแลกเปลี่ยนแต่แท้จริงแล้ว อาจไม่มีการค้าอัตราแลกเปลี่ยนเกิดขึ้นก็ได้ อย่างไรก็ตาม เงินจำนวนดังกล่าวท้ายที่สุดแล้ว ลูกค้าหรือประชาชนที่ลงทุนนั้นจะต้องสูญเสียเงินที่โอนทั้งหมด โดยลูกค้าจะไม่สามารถติดตามเงินที่ลงทุนได้ และบริษัทที่ดำเนินกิจการประเภทนี้จะปิดตัวลง

2.4.2.2.4 การโอนเงินจากบัญชีในกลุ่มเดียวกันเพื่อระดมทุนในการทำการปั่นราคาการซื้อขายหุ้น เพื่อค้ากำไรจากส่วนต่างของราคาหุ้น และหลอกลวงนักลงทุนรายอื่นให้หลงเชื่อในการซื้อหุ้นในราคาที่ได้ปั่นไว้

การโอนเงินผ่านของบัญชีของบุคคลหลายๆ คน แต่บัญชีดังกล่าวเป็นของบุคคลกลุ่มเดียวกัน โดยบุคคลในกลุ่มนั้นจะทำการโอนเงินจากแต่ละบัญชีในการซื้อขายหุ้นหรือหลักทรัพย์ตัวเดียวกันทุกๆ วันเพื่อปั่นราคาหุ้นหรือหลักทรัพย์ดังกล่าวให้มีมูลค่าสูงขึ้น ซึ่งเมื่อมูลค่าหุ้นหรือหลักทรัพย์ดังกล่าวได้ราคาเป็นที่น่าพอใจแล้ว กลุ่มบุคคลดังกล่าวจะทำ

---

[25] นายปรพล สุกาวิน. "กลลวงธุรกิจค้าเงินเถื่อนอันตรายยุคไอเอ็มเอฟ" สคบ.สาร. (ปี 21 : ฉบับที่ 222) : 3-5.

การเทขายหุ้นหรือหลักทรัพย์ที่ถืออยู่ทั้งหมดออกไป และกลุ่มบุคคลนั้นจะได้กำไรจากส่วนต่างของราคามูลค่าหุ้นหรือหลักทรัพย์นั้น ณ วันแรกที่ซื้อขายกับราคาของมูลค่าหุ้น ณ วันที่หุ้นหรือหลักทรัพย์ดังกล่าวมีราคาเป็นที่น่าพอใจ ยกตัวอย่างเช่น วันแรก บัญชีที่ 1 ของนาย ก. โอนเงินเพื่อทำการซื้อหุ้นของบริษัทA ที่ราคาหุ้นละ 20 บาท จำนวน 1,000,000 หุ้น วันที่ 2 บัญชีที่ 2 ของนาย ก. โอนเงินเพื่อซื้อหุ้นของบริษัทA ที่ราคาหุ้นละ 30 บาท วันที่ 3 บัญชีที่ 3 ของนาย ก.โอนเงินเพื่อซื้อหุ้นของบริษัทA ที่ราคาหุ้นละ 40 บาท จนกระทั่งที่บัญชีที่ 5 ของนาย ก. ปั่นราคาหุ้นของบริษัทA ให้อยู่ที่ราคา 70 บาท หลังจากนั้น นาย ก. จะทำการเทขายหุ้นของบริษัท A ที่มีทั้งหมดให้แก่นักลงทุนรายอื่นในราคาหุ้นละ 70 บาท นาย ก. จะได้กำไรจากส่วนต่างของราคาหุ้นๆ ละ 50 บาท ซึ่งจำนวน 1,000,000 หุ้น ณ ราคาขาย 70 บาท นาย ก. จะได้กำไรจากการปั่นราคาหุ้นดังกล่าวจำนวน 50,000,000 บาท และนักลงทุนรายอื่นที่ซื้อหุ้นดังกล่าวจะถูกหลอกลวงให้หลงเชื่อในการซื้อหุ้นที่ปั่นราคาไว้ ซึ่งราคามูลค่าหุ้นที่ซื้อขายดังกล่าวย่อมไม่ใช่ราคามูลค่าหุ้นที่แท้จริง[26]

จากที่กล่าวมาข้างต้นจะเห็นได้ว่า อาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์มีทั้งการกระทำที่มีลักษณะเป็นอาชญากรรมคอมพิวเตอร์และอาชญากรรมที่อาศัยกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในการกระทำความผิดในรูปแบบต่าง ๆ ที่เปรียบเสมือนกับการดำเนินธุรกิจ หรือการดำเนินธุรกรรมทางการเงินการธนาคารโดยปกติทั่วไปประกอบกับการตรวจสอบหรือการป้องกัน หรือการดำเนินการใดๆ รวมถึงการพิสูจน์การกระทำความผิดในการกระทำดังกล่าวจึงมีความยุ่งยากและซับซ้อนมากกว่าอาชญากรรมธรรมดาไม่ว่าจะเป็นเทคโนโลยีที่มีความเกี่ยวข้องกับระบบอิเล็กทรอนิกส์โดยเฉพาะ หรือเป็นอาชญากรรมที่อาศัยการโอนเงินทางอิเล็กทรอนิกส์ในการเป็นเครื่องมือในการฟอกเงินในความผิดลักษณะต่างๆ หรือเงินที่ได้มาหรือได้ประโยชน์จากอาชญากรรมขององค์กรอาชญากรรมข้ามชาติ หรืออาศัยการโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการหลบเลี่ยงฐานภาษี หรือเป็นเครื่องมือในการค้าค่าเงินโดยการแลกเปลี่ยนเงินตราต่างประเทศ ซึ่งอาชญากรรมในแต่ละลักษณะเหล่านี้สามารถสร้างความเสียหายแต่ระบบการเงินการธนาคาร หรือเสถียรภาพทางด้านเศรษฐกิจของประเทศ และส่งผลกระทบต่อความมั่นคงของประเทศชาติได้

---

[26] คดีประวัติศาสตร์ "เสี่ยสองปั่นหุ้น".(ม.ป.ท.),(ม.ป.ป.),หน้า 150.

2.5 ปัญหาและอุปสรรคในการบังคับใช้กฎหมายกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

2.5.1 ปัญหาและอุปสรรคเกี่ยวกับบทบัญญัติแห่งกฎหมายที่ใช้บังคับกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

เนื่องด้วยอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์นั้นมักมีลักษณะของการกระทำที่มีกระบวนการที่ซับซ้อน และสามารถสร้างความเสียหายให้แก่บุคคล นิติบุคคล สถาบันทางเงิน ผู้ที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ หรืออาจสร้างความเสียหายต่างๆ ต่อประเทศชาติ ซึ่งหากพิจารณาถึงความเสียหายต่างๆ ที่กล่าวข้างต้นนั้นอาจเป็นความเสียหายที่มีมูลค่าสูง หรือเป็นความเสียหายต่อระบบเศรษฐกิจ มหภาคหรือเสถียรภาพของระบบการเงินการธนาคารหรือความมั่นคงของประเทศ ซึ่งมูลค่าแห่งความเสียหายต่างๆ ที่เกิดขึ้นอาจเป็นจำนวนที่ไม่อาจเทียบเคียงได้ หรือมีมูลค่ามหาศาล หรือสามารถสร้างผลประโยชน์เป็นจำนวนเงินที่มีมูลค่าสูงมากและดูเหมือนจะเป็นจำนวนเงินที่คุ้มค่าต่อความเสี่ยงในกฎหมายที่ใช้บังคับอยู่ในปัจจุบัน ด้วยเหตุว่ากฎหมายที่บังคับใช้อยู่ในปัจจุบันยังมีข้อจำกัด หรือช่องว่างในการบังคับใช้กับอาชญากรรมที่เกิดขึ้นในแต่ละกรณีอยู่มากพอสมควรหรือหากพิจารณาถึงมาตรการทางกฎหมายอาญาในการบังคับใช้กับผู้กระทำความผิดในลักษณะต่างๆ ที่กล่าวข้างต้นในประเทศไทยยังไม่มีมาตรการทางอาญาในการบังคับใช้กับอาชญากรรมต่างๆ ดังกล่าวไว้โดยตรง

อย่างไรก็ตาม หากพิจารณาถึงกฎหมายที่ใช้บังคับกับการดำเนินงานธนาคารพาณิชย์ หรือกฎหมายที่เกี่ยวข้องกับการเงินการธนาคารที่ใช้บังคับอยู่ในปัจจุบัน ไม่ว่าจะเป็น**พระราชบัญญัติเงินตรา พ.ศ. 2501, พระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485, พระราชบัญญัติการธนาคารพาณิชย์ พ.ศ. 2505, พระราชบัญญัติการธนาคารพาณิชย์ (ฉบับที่ 2) พ.ศ. 2522 และพระราชบัญญัติการธนาคารพาณิชย์ (ฉบับที่ 3) พ.ศ. 2535** นั้นยังไม่มีกฎหมายฉบับใดในการกำหนดมาตรการทางกฎหมายเพื่อบังคับใช้กับอาชญากรรมที่เกิดขึ้นในระบบการโอนเงินทางอิเล็กทรอนิกส์ หรือกระบวนการโอนเงินทางอิเล็กทรอนิกส์ไว้โดยตรง

ด้วยเหตุนี้หากพิจารณาถึงมาตรการทางกฎหมายที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์จึงต้องพิจารณาจากกฎหมายแต่ละฉบับที่กำหนดลักษณะของฐานความผิดไว้เพื่อปรับใช้ในการใช้บังคับกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์อยู่ในปัจจุบัน

2.5.1.1 ปัญหาและอุปสรรคในการบังคับใช้กฎหมายกับอาชญากรรมที่เป็นการกระทำโดยตรงต่อเครื่องหรือระบบอิเล็กทรอนิกส์

หากพิจารณากฎหมายที่บังคับใช้กับอาชญกรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ที่เกิดขึ้นในประเทศไทยนั้นจะเห็นได้ว่า ยังไม่มีมาตรการทางกฎหมายอาญาที่บังคับกับใช้กฎหมายกับอาชญากรรมดังกล่าวไว้โดยตรง ดังนั้นหากพิจารณาการบังคับใช้มาตรการทางกฎหมายกับอาชญากรรมที่เป็นกระทำต่อเครื่องหรือระบบโอนเงินอิเล็กทรอนิกส์หรืออาศัยระบบการโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิดจึงต้องพิจารณาจากกฎหมายหลายฉบับ ไม่ว่าจะเป็น ฐานความผิดลักษณะต่างๆ ของประมวลกฎหมายอาญาซึ่งสามารถพิจารณาและวิเคราะห์ถึงความผิดแต่ละลักษณะที่อาจต้องปรับเพื่อใช้บังคับกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ หรือกฎหมายพิเศษฉบับอื่นๆ

2.5.1.1.1 ประมวลกฎหมายอาญาไทย

หากพิจารณาถึงบทบัญญัติในประมวลกฎหมายอาญา ซึ่งเป็นกฎหมายหลักที่ใช้บังคับกับอาชญากรรมต่างๆ ที่เกิดขึ้นในปัจจุบันกับอาชญากรรมที่เป็นการกระทำต่อเครื่องคอมพิวเตอร์หรือระบบโอนเงินทางอิเล็กทรอนิกส์ในแต่ละความผิดลักษณะต่าง ๆ ซึ่งจะเห็นได้ว่าบทบัญญัติดังกล่าวไม่มีบทบัญญัติในการบังคับใช้กับการกระทำต่อเครื่องคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ไว้โดยตรง ดังนั้นการบังคับใช้กฎหมายกับอาชญากรรมในกรณีดังกล่าวจึงมีข้อควรพิจารณาหลายประการ

<u>ประการแรก</u> การเจาะข้อมูลอิเล็กทรอนิกส์ หรือการดักฟังข้อมูลอิเล็กทรอนิกส์ หรือการขโมยรหัสผ่านในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ เพื่อทำการโอนเงินทางอิเล็กทรอนิกส์นั้นถือเป็นการกระทำที่ครบองค์ประกอบของความผิดฐานลักทรัพย์ ตามประมวลกฎหมายอาญาหรือไม่ ซึ่งการวิเคราะห์ประเด็นดังกล่าวอาจต้องพิจารณาว่าการเจาะหรือการดักฟังหรือการขโมยเข้าข่ายที่อยู่ในองค์ประกอบของการเอาไปเสีย หรือข้อมูลอิเล็กทรอนิกส์หรือรหัสผ่านที่ใช้ในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ต้องถือเป็นทรัพย์ตามประมวลกฎหมายอาญา[27]

---

[27] <u>ประมวลกฎหมายอาญา</u>, มาตรา 334.

ผู้ใดเอาทรัพย์ของผู้อื่น หรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วยไปโดยทุจริต ผู้นั้นกระทำความผิดฐานลักทรัพย์ ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินหกพันบาท

<u>ประการที่สอง</u> การทำลายโปรแกรมคอมพิวเตอร์ที่ใช้ในการตรวจสอบความถูกต้องของระบบโอนเงินทางอิเล็กทรอนิกส์เพื่อประโยชน์ในการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งการวิเคราะห์ประเด็นนี้จะต้องถือว่าการกระทำต่อโปรแกรมคอมพิวเตอร์ หรือข้อมูลอิเล็กทรอนิกส์ดังกล่าวเป็นการกระทำในลักษณะการทำให้เสียทรัพย์ และโปรแกรมคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์นั้นเป็นทรัพย์ตามประมวลกฎหมายอาญา[26]

<u>ประการที่สาม</u> การปลอมแปลงข้อมูลอิเล็กทรอนิกส์ หรือรหัสผ่านเพื่อพลวกลวงระบบโอนเงินทางอิเล็กทรอนิกส์ โดยข้อมูลอิเล็กทรอนิกส์ดังกล่าวหรือรหัสผ่านที่ใช้ในกระบวนการโอนเงินทางอิเล็กทรอนิกส์เป็นเงื่อนไขสำคัญ ในการทำให้ระบบโอนเงินทางอิเล็กทรอนิกส์ส่งคำสั่งโอนเงินทางอิเล็กทรอนิกส์นั้นตามต้องการ ซึ่งกรณีนี้จึงต้องพิจารณาว่าการกระทำดังกล่าวจัดเป็นการกระทำความผิดฐานปลอมเอกสารสิทธิ[29] และใช้เอกสารปลอม[30]ตามประมวลกฎหมายอาญา ประกอบการพิจารณาว่าข้อมูลอิเล็กทรอนิกส์จัดเป็นเอกสารสิทธิตามประมวลกฎหมายอาญา[31]

<u>ประการที่สี่</u> การแจ้งข้อความอันเป็นเท็จหรือข้อความไม่ตรงต่อความจริงต่อระบบโอนเงินทางอิเล็กทรอนิกส์ เพื่อฉ้อโกงรายการทางบัญชีของบุคคลอื่นให้มีการโอน

---

[28] <u>ประมวลกฎหมายอาญา.</u>,มาตรา 358.

ผู้ใดทำให้เสียหาย ทำลาย ทำให้เสื่อมค่าหรือทำให้ไร้ประโยชน์ ซึ่งทรัพย์ของผู้อื่นหรือผู้อื่นเป็นเจ้าของรวมอยู่ด้วย ผู้นั้นกระทำความผิดฐานทำให้เสียทรัพย์ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ

[29] เรื่องเดียวกัน.,มาตรา 265.

ผู้ใดปลอมเอกสารสิทธิหรือเอกสารราชการ ต้องระวางโทษจำคุกตั้งแต่หกเดือนถึงห้าปี และปรับตั้งแต่หนึ่งพันบาทหรือหนึ่งหมื่นบาท

[30] เรื่องเดียวกัน.,มาตรา 268.

ผู้ใดใช้หรืออ้างเอกสารอันเกิดจากการกระทำความผิดตามมาตรา 264 มาตรา 265 มาตรา 266 หรือมาตรา 267 ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษดังที่บัญญัติไว้ในมาตรานั้นๆ

[31] เรื่องเดียวกัน.,มาตรา 1 (9).

"เอกสารสิทธิ" หมายความว่า เอกสารที่เป็นหลักฐานแห่งการก่อ เปลี่ยนแปลง โอน สงวน หรือการระงับซึ่งสิทธิ

เงินจากบัญชีดังกล่าวมาสู่บัญชีของตนภายใต้กระบวนการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งกรณีนี้จะต้องพิจารณาว่าการแจ้งข้อความอันเป็นเท็จหรือการแจ้งข้อความไม่ตรงต่อความจริง เพื่อให้ได้มาซึ่งการโอนเงินทางอิเล็กทรอนิกส์นั้นเป็นการกระทำความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา[32]

หากพิจารณาถึง ปัญหาและอุปสรรคในการบังคับใช้ประมวลกฎหมายอาญาดังกล่าวกับอาชญากรรมที่เป็นการกระทำต่อระบบโอนเงินทางอิเล็กทรอนิกส์ที่บังคับใช้กับบทบัญญัติในประมวลกฎหมายอาญาปัจจุบันนั้นจะเห็นได้ว่ามีปัญหาและอุปสรรคหลายประการกล่าวคือ

1. บทบัญญัติดังกล่าวได้บัญญัติถึงลักษณะของฐานการกระทำความผิดที่ไม่ครอบคลุมถึงอาชญากรรมที่อาศัยข้อมูลทางอิเล็กทรอนิกส์ รหัสผ่าน หรือโปรแกรมทางคอมพิวเตอร์ไว้โดยตรง

2. บทกำหนดโทษในแต่ละลักษณะความผิดแล้วยังมีความล้าหลังและไม่สมดุลกับความเสียหายที่เกิดขึ้นกับอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในปัจจุบัน

3. การบังคับใช้กฎหมายตามประมวลกฎหมายอาญากับอาชญากรรมในแต่ละลักษณะดังกล่าวนั้นต้องอาศัยการตีความเพื่อเทียบเคียงกับฐานความผิดต่างๆ ในประมวลกฎหมายอาญา ซึ่งมิได้มีการบัญญัติในแต่ละลักษณะความผิดดังกล่าวไว้โดยตรง ประเด็นดังกล่าวจึงเป็นความขัดแย้งในการบังคับใช้กฎหมายดังกล่าวได้ เนื่องจากหลักการพื้นฐานทางอาญา (NULLUM CRIMAN NULLA POENA) ได้กำหนดว่า ความผิดและการลงโทษกระทำได้ก็ต่อเมื่อมีกฎหมายบัญญัติไว้ และหลักการดังกล่าวได้บัญญัติไว้ในมาตรา 2 แห่งประมวลกฎหมายอาญาเช่นกัน ดังนั้นการตีความโดยเทียบเคียงกับฐานความผิดตามประมวลกฎหมายอาญา เพื่อบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าวจึงอาจมีความขัดแย้งของการบังคับใช้กฎหมายว่าเป็นการตีความเพื่อบังคับใช้กฎหมายดังกล่าวเป็นการตีความที่ขัดกับหลักการพื้นฐานทางอาญาหรือไม่

4. พยานหลักฐานทางอิเล็กทรอนิกส์เป็นประเด็นสำคัญด้านพยานหลักฐานในการใช้เสนอต่อศาล เพื่อเป็นพยานหลักฐานในการบังคับใช้กฎหมายกับอาชญากรรมใน

---

[32] ประมวลกฎหมายอาญา, มาตรา 341

ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความซึ่งควรบอกให้แจ้งและโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม ...ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ

ลักษณะดังกล่าว ซึ่งตามประมวลกฎหมายวิธีพิจารณาความอาญาปัจจุบันยังไม่มีบทบัญญัติที่กำหนดถึง หลักเกณฑ์ในการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ไว้อย่างชัดเจนนัก และปัจจุบันยังเป็นปัญหาในการรับฟังพยานหลักฐานว่า พยานหลักฐานทางอิเล็กทรอนิกส์เป็นพยานหลักฐานที่รับฟังได้ในฐานะพยานเอกสารหรือพยานบอกเล่า ซึ่งการชั่งน้ำหนักในการรับฟังพยานหลักฐานที่กล่าวข้างต้นนี้มีน้ำหนักในการรับฟังพยานหลักฐานที่แตกต่างกัน

5. หน่วยงานหรือมาตรการในการเก็บรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ เพื่อเป็นมาตรการในการรองรับกระบวนวิธีพิจารณาทางอาญาที่ใช้ในการดำเนินคดีกับอาชญากรรมดังกล่าวไว้โดยเฉพาะ

2.5.1.1.2 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

หากพิจารณาการบังคับใช้กฎหมาย ตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544 กับอาชญากรรมที่เป็นการกระทำต่อเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์นั้นมีข้อควรพิจารณา กล่าวคือ พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544 มีวัตถุประสงค์ในการตราพระราชบัญญัติฉบับนี้ขึ้น เพื่อรองรับสถานะทางกฎหมายของธุรกรรมทางอิเล็กทรอนิกส์ที่เกิดขึ้นอย่างแพร่หลายในปัจจุบัน ซึ่งการทำธุรกรรมประเภทต่างๆ ได้มีการพัฒนาโครงข่ายการติดต่อสื่อสารทางด้านเทคโนโลยีอิเล็กทรอนิกส์ที่มีความสะดวกรวดเร็ว และสามารถเชื่อมโยงเครือข่ายการติดต่อสื่อสารระหว่างกันได้อย่างกว้างขวางทั่วโลก เพื่อนำมาใช้ในการทำธุรกรรมประเภทต่างๆ หรือที่เรียกกันโดยทั่วไปว่า"ธุรกรรมอิเล็กทรอนิกส์" ซึ่งประเด็นที่ต้องพิจารณาว่าพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ฉบับนี้ มีบทบัญญัติในการบังคับใช้กับอาชญากรรมที่กระทำต่อเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์หรือไม่ กล่าวคือ

<u>ประการแรก</u> ธุรกรรมอิเล็กทรอนิกส์เป็นธุรกรรมที่มีวิธีการที่แตกต่างจากธุรกรรมโดยทั่วไป กล่าวคือ การทำธุรกรรมอิเล็กทรอนิกส์ หมายถึง ธุรกรรมที่ต้องกระทำขึ้นโดยวิธีการทางอิเล็กทรอนิกส์ทั้งหมด หรือแต่บางส่วนโดยอาจจะกระทำผ่านทางเครือข่ายอินเทอร์เน็ตหรือวิธีการทางอิเล็กทรอนิกส์อื่นๆ อาทิเช่น โทรเลข การพิมพ์ หรือโทรสาร ก็ได้[33] ซึ่งประเด็นที่ต้องพิจารณาถึงการโอนเงินทางอิเล็กทรอนิกส์ถือเป็นธุรกรรมทางอิเล็กทรอนิกส์ตาม

---

[33] ชัยวัฒน์ วงศ์วัฒนศานต์ ทวีศักดิ์ กออนันตกูล และสุรางคณา แก้วจำนงค์. <u>คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544</u>.(จิรรัชกิจการพิมพ์ :กรุงเทพมหานคร ,2544), หน้า 59.

ความหมายในการทำธุรกรรมทางอิเล็กทรอนิกส์แห่งพระราชบัญญัติฉบับนี้หรือไม่ ซึ่งกฎหมายฉบับนี้ได้กำหนดขอบเขตในการบังคับใช้ไว้ให้ใช้บังคับได้เป็นการทั่วไป โดยมุ่งหมายให้ใช้บังคับกับธุรกรรมทางแพ่งและพาณิชย์ที่ใช้ข้อมูลทางอิเล็กทรอนิกส์ เว้นแต่ธุรกรรมบางประเภทที่พระราชกฤษฎีกากำหนด โดยมิให้นำพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับ[34]

หากพิจารณาถึงความหมายของคำว่า "ธุรกรรมทางอิเล็กทรอนิกส์" และ "ธุรกรรม" ตามมาตรา 4 [35] แห่งพระราชบัญญัติฉบับนี้ หมายถึง ธุรกรรมที่กระทำขึ้นโดยวิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน และคำว่า "ธุรกรรม" รวมถึงการกระทำใดๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของภาครัฐด้วย

ดังนั้นหากพิจารณาความหมายของคำว่า "ธุรกรรม" และ "ธุรกรรมทางอิเล็กทรอนิกส์" ตามที่ได้อธิบายแล้วข้างต้น คำว่า "ธุรกรรมทางอิเล็กทรอนิกส์" หมายถึง การกระทำใด ๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ ซึ่งได้กระทำขึ้นโดยวิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน ดังนั้น จึงมีประเด็นที่ต้องพิจารณาว่าธุรกรรมทางอิเล็กทรอนิกส์จะสามารถครอบคลุมถึงการโอนเงินทางอิเล็กทรอนิกส์ได้ทุกประเภทหรือไม่ แม้ว่าการโอนเงินทางอิเล็กทรอนิกส์จะเป็นกระบวนการหนึ่งภายใต้ระบบอิเล็กทรอนิกส์ แต่การโอนเงินในแต่ละกรณีจะถือได้ว่าเป็นกิจกรรมในทางแพ่งและพาณิชย์หรือไม่ ซึ่งโดยทั่วไปการโอนเงินทางอิเล็กทรอนิกส์มักจะมีวัตถุประสงค์ในทางแพ่งและพาณิชย์รองรับ ไม่ว่าจะเป็นการโอนเงินเพื่อชำระราคา หรือมีวัตถุประสงค์ในการชำระหนี้ และความสัมพันธ์ในการโอนเงินทางอิเล็กทรอนิกส์ในทางปฏิบัติทั่วไปนั้นจะเป็นความสัมพันธ์ระหว่างธนาคารกับผู้โอนหรือผู้รับโอน ซึ่งผู้ให้บริการทางการโอนเงินทางอิเล็กทรอนิกส์ได้พยายามนำกฎหมายแพ่งและพาณิชย์ที่มีอยู่ในปัจจุบันมาปรับใช้กับกรณีดังกล่าว เช่น กฎหมายลักษณะสัญญา กฎหมายลักษณะตัวแทน เป็นต้น แต่ยังมีประเด็นในการตีความว่ากฎหมายดังกล่าวซึ่งยังไม่ชัดเจนเพียงพอ และไม่สามารถครอบคลุมทุกกรณีที่อาจจะมีปัญหาเกิดขึ้นได้[36]

---

[34]ชัยวัฒน์ วงศ์วัฒนศานต์ ทวีศักดิ์ กออนันตกูล และสุรางคณา แก้วจำนงค์. คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544., (จิรรัชการพิมพ์ : กรุงเทพมหานคร ,2544), หน้า 14.

[35] เรื่องเดียวกัน.หน้า 154.

[36] สายวิเคราะห์ ฝ่ายระบบการชำระเงิน ธนาคารแห่งประเทศไทย.เอกสารประกอบการสัมมนาเกี่ยวกับกฎหมายว่าด้วยการโอนเงินทางอิเล็กทรอนิกส์. "แนวคิดเรื่องกฎหมายการโอนเงินทางอิเล็กทรอนิกส์".(ม.ป.ท.),(ม.ป.ป.),หน้า 5.

หากพิจารณาถึง การโอนเงินทางอิเล็กทรอนิกส์ที่ไม่อาจนำกฎหมายแพ่งและพาณิชย์มาปรับใช้ได้นั้น ถือได้ว่าเป็นการโอนเงินทางอิเล็กทรอนิกส์ที่ไม่มีความสัมพันธ์ทางแพ่งและพาณิชย์รองรับ เช่น การโอนเงินเพื่อให้มีความเคลื่อนไหวทางบัญชีโดยมิได้มีวัตถุประสงค์ในการก่อ เปลี่ยนแปลง โอน สงวน ระงับ ซึ่งสิทธิแห่งเงินดังกล่าวแต่อย่างใด แต่มีวัตถุประสงค์เพียงการเคลื่อนย้ายเงินในบัญชี และมิได้มีการเปลี่ยนแปลงซึ่งนิติสัมพันธ์หรือสิทธิและหน้าที่ระหว่างกันแต่อย่างใด อีกทั้งความสัมพันธ์ระหว่างผู้โอนเงินกับผู้รับโอนเงินทางการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าวยังคงไม่เปลี่ยนแปลง โดยความสัมพันธ์ของสิทธิและหน้าที่ระหว่างผู้โอนเงินกับผู้รับโอนในเงินจำนวนดังกล่าวยังเป็นสิทธิและหน้าที่ที่มีอยู่ในบุคคลคนเดียวกัน และสิทธิหน้าที่ของธนาคารก็มีเพียงหน้าที่ในการปฏิบัติตามคำสั่งของผู้โอนเงินและผู้รับโอนเงินเท่านั้น ซึ่งเป็นปัญหาในการพิจารณาได้ว่า การโอนเงินทางอิเล็กทรอนิกส์ที่มิได้มีวัตถุประสงค์ในการชำระเงินหรือเป็นเพียงการเคลื่อนย้ายเงินในบัญชีของตนเองเท่านั้นจึงมิใช่การโอนเงินที่มีวัตถุประสงค์ที่มีกิจกรรมทางแพ่งและพาณิชย์รองรับอยู่ ดังนั้น ประเด็นนี้จึงยังคงเป็นปัญหาในการบังคับใช้กฎหมายตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ว่าสามารถบังคับใช้กับการโอนเงินทางอิเล็กทรอนิกส์ได้ในทุกกรณีหรือไม่

ทั้งนี้ หากจะกล่าวถึงปัญหาและอุปสรรคสำคัญในการบังคับใช้กฎหมายกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งบทบัญญัติแห่งพระราชบัญญัติฉบับนี้มิได้วางบทบัญญัติในการบังคับใช้กับการกระทำโดยๆ โดยทุจริต ไม่ว่าจะเป็นอาชญากรรมที่มีลักษณะแห่งการกระทำเป็นการกระทำต่อเครื่อง หรือกระบวนการโอนเงินทางอิเล็กทรอนิกส์เพื่อให้ได้มาซึ่งประโยชน์โดยมิชอบหรือที่เรียกว่า"อาชญากรรมคอมพิวเตอร์" หรือการใช้การโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการแสวงหาผลประโยชน์ลักษณะต่าง ๆ โดยทุจริต ซึ่งพระราชบัญญัติฉบับนี้มิได้มีบทบัญญัติในการบังคับใช้กฎหมายกับการกระทำความผิดแต่ละลักษณะดังกล่าวไว้แต่อย่างใด

ด้วยเหตุนี้ หากพิจารณาถึงหลักการสำคัญของพระราชบัญญัติฉบับนี้กล่าวคือ พระราชบัญญัติฉบับนี้มีวัตถุประสงค์ในการวางบทบัญญัติเพื่อรองรับสถานะของการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีสถานะทางกฎหมาย หรือให้ข้อมูลทางอิเล็กทรอนิกส์ที่เกิดขึ้นในธุรกรรมทางอิเล็กทรอนิกส์มีผลใช้บังคับได้ในทางกฎหมาย เพื่อรองรับความสมบูรณ์ของธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าว แต่พระราชบัญญัติฉบับนี้ยังมิได้กำหนดบทบัญญัติในการบังคับใช้กับอาชญากรรมที่เกิดขึ้นต่อธุรกรรมอิเล็กทรอนิกส์ หรือกระบวนการโอนเงินทางอิเล็กทรอนิกส์ไว้แต่อย่างใด

2.5.1.1.3. ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์

ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ เป็นส่วนหนึ่งของโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ซึ่งขณะนี้ร่างกฎหมายฉบับดังกล่าวอยู่ระหว่างการนำเสนอคณะรัฐมนตรีเพื่อพิจารณาโดยมีเนื้อหาสาระครอบคลุมถึงอาชญากรรมทางคอมพิวเตอร์ที่เป็นการกระทำความผิดซึ่งกำหนดฐานความผิดลักษณะต่างๆ ที่เป็นความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ไว้โดยเฉพาะ ไม่ว่าจะเป็น ความผิดการเข้าถึงโดยไม่มีอำนาจ หรือ การใช้คอมพิวเตอร์โดยมิชอบ ซึ่งในกฎหมายฉบับนี้ได้กำหนดถึงฐานความผิด การลักลอบดักข้อมูลโดยฝ่าฝืนกฎหมาย การรบกวนข้อมูล การรบกวนระบบ หรือความผิดที่เกี่ยวข้องกับคอมพิวเตอร์

หากพิจารณาถึงฐานความผิดของร่างกฎหมายฉบับดังกล่าว มีรายละเอียดของแต่ละฐานความผิดสรุปโดยสังเขป[37] ดังนี้

1. ความผิดฐาน "การเข้าถึงโดยไม่มีอำนาจ" หมายถึง การเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วน โดยประการที่น่าจะเป็นเหตุให้เกิดความเสียหายหรือรบกวนการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือระบบข้อมูล
2. "การลักลอบดักข้อมูล" หมายถึง การลักลอบดักข้อมูลของผู้อื่นจากระบบข้อมูล ระบบคอมพิวเตอร์ หรือที่ส่งผ่านระบบคอมพิวเตอร์หรือระบบเครือข่าย ซึ่งเพื่อให้ได้มาซึ่งข้อมูลทางคอมพิวเตอร์ โดยวิธีการทางเทคนิค หรือแอบบันทึกข้อมูลที่สื่อสารทางอิเล็กทรอนิกส์
3. "การรบกวนระบบ" หมายถึง การรบกวน ขัดขวาง แทรกแซง หรือหยุดการทำงานของระบบคอมพิวเตอร์ ระบบข้อมูล หรือระบบเครือข่าย โดยการนำเข้า ส่ง ทำลาย ลบ ทำให้เสื่อมประโยชน์ ทำให้เสียประโยชน์ เปลี่ยนแปลงข้อมูลคอมพิวเตอร์ ย้าย หรือแก้ไขระบบข้อมูล
4. "การผลิต จำหน่าย มีอุปกรณ์เพื่อใช้ในการกระทำความผิด" หมายถึง การผลิต แจกจ่าย ขาย เสนอขาย แลกเปลี่ยน เสนอแลกเปลี่ยน

---

[37] ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ.... และ ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ....., (จิรรัชการพิมพ์ : กรุงเทพมหานคร, 2544), หน้า 28.

ส่งออก จัดซื้อ ใช้หรือจัดให้มีซึ่งเครื่องคอมพิวเตอร์ เครื่องมืออิเล็กทรอนิกส์ โปรแกรมคอมพิวเตอร์ เครื่องมือในลักษณะคล้ายคลึงกัน รหัสผ่านเครื่องคอมพิวเตอร์ รหัสการเข้าถึงข้อมูลอันทำให้เข้าถึงระบบคอมพิวเตอร์ ระบบข้อมูลแม้แต่เพียงส่วนหนึ่งส่วนใดเพื่อใช้ในการกระทำความผิด

5. "ความผิดต่อการครอบครองโปรแกรมคอมพิวเตอร์ไว้ใช้ในการกระทำความผิด" หมายถึง การครองครอง หรือควบคุมโปรแกรม ข้อมูล หรือข้อความซึ่งอยู่ในคอมพิวเตอร์ หรือเรียกดูโปรแกรม ข้อมูล หรือข้อความจากคอมพิวเตอร์เครื่องใดเครื่องหนึ่งโดยไม่มีอำนาจ
6. "ความผิดต่อการปลอมแปลง" หมายถึง การปลอมข้อมูลขึ้นทั้งหมดหรือแต่ส่วนหนึ่งส่วนใด แปลง เติมหรือตัดทอนข้อมูล หรือแก้ไขข้อมูลที่แท้จริง หรือประทับตราปลอม หรือปลอมลายมือชื่ออิเล็กทรอนิกส์ในข้อมูล หรือรบกวนการทำงานของระบบคอมพิวเตอร์ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน และเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นข้อมูลที่แท้จริง โดยไม่คำนึงว่าข้อมูลนั้นจะสามารถอ่านออกหรือแม้ไม่สามารถเข้าใจได้ก็ตาม
7. "ความผิดฐานฉ้อโกง" หมายถึง การกระทำโดยทุจริต เติมข้อความอันเป็นเท็จ ตัดหรือแก้ไขด้วยประการใดๆ ในข้อมูลที่แท้จริงของผู้อื่น หรือกระทำการรบกวนการทำงานของระบบข้อมูลหรือระบบคอมพิวเตอร์ของผู้อื่น และการกระทำเช่นว่านั้นทำให้ได้ทรัพย์หรือประโยชน์จากผู้อื่น หรือทำให้ผู้อื่นทำ ถอน หรือทำลายสิทธิ ถือว่าเป็นความผิดฐานฉ้อโกงคอมพิวเตอร์
8. "ความผิดฐานจารกรรมหรือก่อการร้าย" หมายถึง กระทำการใดๆ ในการจารกรรมข้อมูล เพื่อให้ตนได้ข้อมูลหรือเข้าถึงข้อมูลซึ่งมีการรักษาความปลอดภัยไว้เป็นพิเศษโดยประการที่น่าจะส่งผลกระทบต่อความมั่นคงของรัฐ หรือเพื่อก่อการร้ายหรือการสงคราม หรือในทางอื่นอันเป็นปรปักษ์ต่อรัฐ

ทั้งนี้ลักษณะของฐานความผิดตามพระราชบัญญัติฉบับดังกล่าวอาจมีการเปลี่ยนแปลงได้ภายหลังจากที่กฎหมายฉบับนี้ได้ผ่านการพิจารณาจากสภาเป็นที่เรียบร้อยแล้ว

หากพิจารณาถึงฐานความผิดที่กำหนดไว้ในร่างกฎหมายฉบับนี้จะเห็นได้ว่าเป็นบทบัญญัติที่สามารถตีความให้ใช้บังคับกับอาชญากรรมที่เกิดขึ้นกระบวนการโอนเงินทางอิเล็กทรอนิกส์ได้ในกรณีที่อาชญากรรมดังกล่าวเป็นอาชญากรรมที่กระทำต่อระบบ โปรแกรม หรือกระบวนการโอนเงินทางอิเล็กทรอนิกส์โดยตรง หรือเรียกได้ว่าสามารถบังคับใช้ได้กับอาชญากรรมทางคอมพิวเตอร์ที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ได้ หากแต่การบังคับใช้ร่างกฎหมายดังกล่าวกับอาชญากรรมทางคอมพิวเตอร์ที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ต้องอาศัยการตีความว่า คอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ ข้อมูลทางอิเล็กทรอนิกส์ตามร่างกฎหมายฉบับนี้ รวมถึง คอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ หรือข้อมูลทางอิเล็กทรอนิกส์ของในการโอนเงินทางอิเล็กทรอนิกส์ภายใต้ระบบการเงินการธนาคารหรือสถาบันทางการเงินด้วย

อย่างไรก็ตาม การบังคับใช้ร่างกฎหมายฉบับดังกล่าวกับอาชญากรรมที่เกิดขึ้นกระบวนการโอนเงินทางอิเล็กทรอนิกส์ก็ยังไม่อาจรวมถึงอาชญากรรมที่อาศัยการโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิด ไม่ว่าจะเป็น การฟอกเงินผ่านทางการโอนเงินทางอิเล็กทรอนิกส์ การลักลอบโอนเงินออกนอกประเทศเพื่อซื้อขายหรือแลกเปลี่ยนเงินตราต่างประเทศโดยไม่ได้รับอนุญาต หรือการลักลอบโอนเงินออกนอกประเทศเพื่อหลีกเลี่ยงฐานภาษี เป็นต้น

2.5.1.2 ปัญหาและอุปสรรคในการบังคับใช้กฎหมายกับอาชญากรรมที่ใช้หรือนำระบบโอนเงินทางอิเล็กทรอนิกส์มาใช้เป็นเครื่องมือในการกระทำความผิด หรือแสวงหาประโยชน์โดยมิชอบหรือโดยทุจริต

การซื้อขายแลกเปลี่ยนเงินตราต่างประเทศ ซึ่งอยู่ภายใต้การควบคุมของพระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485 มาตรา 8 ทวิ ประกอบกับพระราชบัญญัติศุลกากร พ.ศ. 2469 มาตรา 27 เรื่องการสั่งห้ามนำเข้า ส่งออกของต้องกำกัด ซึ่งกรณีดังกล่าวมีความผิดและกรมศุลกากรสามารถริบของดังกล่าวนั้นได้ทันที

หากพิจารณาถึง การกระทำอันเป็นการใช้หรือนำระบบโอนเงินทางอิเล็กทรอนิกส์มาใช้เพื่อลักลอบโอนเงินเพื่อค้าอัตราแลกเปลี่ยนเงินตราต่างประเทศ ซึ่งจะส่งผลสร้างความเสียหายต่อระบบการเงินการธนาคารและเศรษฐกิจมหภาคของประเทศ ดังนั้นปัญหาในการบังคับใช้กฎหมายกับกรณีดังกล่าวในปัจจุบันจะเห็นว่า การซื้อขายแลกเปลี่ยนเงินตราต่างประเทศอยู่ในความควบคุมดูแลของ รัฐมนตรีว่าการกระทรวงการคลังภายใต้พระราชบัญญัติ

ควบคุมการเปลี่ยนเงิน พ.ศ. 2485 ซึ่งแก้ไขเพิ่มเติมโดยพระราชกำหนดแก้ไขเพิ่มเติมพระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน (ฉบับที่ 2) พ.ศ. 2527 โดยให้ถือว่าความผิดดังกล่าวเป็นความผิดตามกฎหมายศุลกากร

2.5.1.2.1 พระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485

พระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน ซึ่งแก้ไขเพิ่มเติมโดยพระราชกำหนดแก้ไขเพิ่มเติมพระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน (ฉบับที่ 2) พ.ศ. 2527 มีขอบเขตในการบังคับใช้ให้ครอบคลุมถึงกรณีของการลักลอบส่งหรือนำเงินตราไทยออกไปนอกหรือเข้ามาในประเทศไทยโดยผิดกฎหมาย ซึ่งทางปฏิบัติเดิมหน่วยงานราชการไทยไม่สามารถริบเงินตราไทยจากบุคคลที่ได้ทำการลักลอบนั้นได้ ด้วยเหตุว่ามีคำพิพากษาฎีกาหลายฉบับพิพากษาว่า ธนบัตรของไทย หรือธนบัตรที่เป็นของกลางมิใช่ "ของ" อันอาจไปจำหน่ายเป็นสินค้าได้อย่างธรรมดาทั่วๆ ไป จึงไม่สามารถริบจากกรณีดังกล่าวได้ ดังนั้น ตามมาตรา 8 ทวิแห่งพระราชบัญญัติฉบับดังกล่าวได้กำหนดให้การป้องกันและปราบปรามการลักลอบส่ง หรือนำเงินออกไปนอกหรือเข้ามาในประเทศไทยให้ถือว่าเงินดังกล่าวเป็นของต้องจำกัด และให้ถือเป็นความผิดตามการส่งหรือนำของต้องกำกัดออกไปนอกหรือเข้ามาในประเทศไทย ตามกฎหมายว่าด้วยศุลกากรด้วย

โดยการนำเข้าหรือส่งออกของต้องกำกัดที่รวมถึงเงิน เงินตราตามกรณีข้างต้นนั้นจะต้องได้รับการปฏิบัติที่ครบถ้วนตามที่ได้กำหนดไว้ในกฎหมายนั้น ไม่ว่าจะเป็นการมีใบอนุญาตการนำเข้าและส่งออก ประกอบหลักฐานรองรับการนำเข้าหรือส่งออกนั้นซึ่งอยู่ในอำนาจ และความควบคุมของรัฐมนตรีว่าการกระทรวงการคลัง ทั้งนี้ หากการนำเข้าและส่งออกเงินออกนอกประเทศโดยไม่ได้ขออนุญาตแล้ว ตามกฎหมายศุลกากรถือได้ว่าเป็นการนำเข้าและส่งออกซึ่งของต้องกำกัดตามความผิดฐานนำของต้องห้ามหรือของต้องกำกัดเข้ามาในหรือส่งออกนอกราชอาณาจักรโดยไม่ได้รับอนุญาต และตามกฎหมายศุลกากรได้กำหนดให้มีความผิดและกำหนดโทษผู้กระทำความผิดดังกล่าวไว้สูงสุด คือ การให้ริบของที่หลีกเลี่ยงข้อห้ามกำกัดทั้งหมดและให้ปรับเป็นจำนวนเงิน 4 เท่าของราคารวมค่าภาษีอากรแล้ว

หากพิจารณาถึงความผิดตามกฎหมายศุลกากร ซึ่งได้กำหนดถึงความผิดเกี่ยวกับการนำของต้องห้ามหรือของต้องกำกัดเข้ามาในหรือส่งออกนอกราชอาณาจักรโดยไม่ได้รับอนุญาตแล้วยังมีความผิดฐานสำแดงเท็จ ซึ่งเป็นความผิดต่อการสำแดงลักษณะใดๆ เกี่ยวกับการนำเข้าหรือส่งออกสินค้าซึ่งไม่ตรงกับหลักฐานเอกสารและข้อเท็จจริงในการนำเข้าและการส่งออก ซึ่งความผิดฐานสำแดงเท็จนี้มีอยู่หลายลักษณะกล่าวคือ

- การยื่นใบขนสินค้า คำสำแดง ใบรับรอง บันทึกเรื่องราว หรือตราสารอย่างอื่นต่อกรมศุลกากรซึ่งเป็นเท็จ
- การไม่ตอบคำถามของเจ้าหน้าที่ศุลกากรที่ปฏิบัติหน้าที่ตามกฎหมายด้วยความสัตย์จริง
- การไม่ยอม หรือละเลย ไม่ทำ ไม่บันทึกเรื่องราวหรือทะเบียนหรือสมุดบัญชีหรือเอกสารหรือตราสารที่กฎหมายศุลกากรกำหนดไว้
- การปลอมแปลงหรือใช้เอกสาร บันทึกเรื่องราว หรือตราสารอย่างอื่นปลอม
- การแก้ไขเอกสาร บันทึกเรื่องราว หรือตราสารอย่างหนึ่งอย่างใดภายหลังที่ราชการออกให้แล้ว

2.5.1.2.2 ข้อกฎหมายและระเบียบเกี่ยวกับการขอซื้อเงินตราต่างประเทศนอกเหนือจากพระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน

กรณีการซื้อเงินตราต่างประเทศต้องปฏิบัติตามประกาศกระทรวงการคลัง เรื่อง คำสั่งรัฐมนตรีให้ไว้แก่ตัวแทนรับอนุญาต ลงวันที่ 19 มีนาคม 2534 ซึ่งประกาศฉบับนี้ได้กำหนดให้การซื้อขายเงินตราต่างประเทศต้องกระทำโดยตัวแทนรับอนุญาต และกำหนดสิทธิและหน้าที่ของตัวแทนรับอนุญาตในการทำการซื้อขายเงินตราต่างประเทศ โดยมีรายละเอียดดังต่อไปนี้

1. ตัวแทนรับอนุญาตต้องดูแลให้ผู้ยื่นใช้แบบคำขอ และแบบรายงานให้ถูกต้องตามที่เจ้าพนักงานกำหนด และให้ผู้ยื่นสำแดงรายการให้ครบถ้วนตามที่ปรากฏในแบบนี้ โดยตัวแทนอนุญาตต้องตรวจและดูแลให้คำขอและแบบรายงานต่าง ๆ เป็นไปตามที่กำหนดในกฎกระทรวง ประกาศกระทรวงการคลัง ประกาศ และคำสั่งเจ้าพนักงาน ทั้งต้องรับผิดชอบว่าการกระทำใด ๆ ตามคำขอหรือรายงานดังกล่าวเป็นไป โดยถูกต้องครบถ้วนตามกฎกระทรวง ประกาศ กระทรวงการคลัง ประกาศและคำสั่งของเจ้าพนักงาน

2. เมื่อตัวแทนรับอนุญาตขายหรือแลกเปลี่ยนเงินตราต่างประเทศตามคำขอใด ให้เป็นตัวแทนรับอนุญาตสำแดงจำนวนเงินที่ขายหรือแลกเปลี่ยนอัตราแลกเปลี่ยนและวันเดือนปีที่ขายหรือแลกเปลี่ยนในคำขอนั้น

3. การขาย หรือการแลกเปลี่ยนเงินตราต่างประเทศให้ตัวแทนรับอนุญาตเป็นผู้เรียกให้ผู้ขอยื่นเอกสารหลักฐานตามที่เจ้าพนักงานกำหนด เมื่อตัวแทนรับอนุญาตตรวจสอบและพอใจว่าเป็นเอกสารที่แท้จริงและถูกต้อง ก็ให้ขาย หรือแลกเปลี่ยนเงินตราต่างประเทศนั้นได้

4. การขาย หรือแลกเปลี่ยนเงินตราต่างประเทศในวงเงินเกินกว่าห้าพันดอลล่าร์สหรัฐอเมริกาหรือเทียบเท่าตามอัตราตลาด ตัวแทนรับอนุญาตจะต้องจัดให้ผู้ขอยื่นรายงานตามแบบ ธ.ต. 4 ด้วย

5. ตัวแทนรับอนุญาตขายหรือแลกเปลี่ยนเงินตราต่างประเทศแล้วให้ปฏิบัติดังนี้

(1) ประทับตราบนเอกสารหลักฐาน และเก็บรักษาเอกสารหลักฐานนั้นไว้ไม่น้อยกว่า 3 ปีเพื่อให้เจ้าพนักงานตรวจสอบเมื่อต้องการ

(2) สำแดงจำนวนเงินที่ขายหรือแลกเปลี่ยน อัตราแลกเปลี่ยน วันเดือนปีที่ขายหรือแลกเปลี่ยนพร้อมทั้งลงลายมือชื่อและประทับตราในแบบ ธ.ต. 4 และส่งแบบ ธ.ต. 4 ดังกล่าวไปให้เจ้าพนักงานภายใน 3 วันทำการ นับแต่วันที่ขายหรือแลกเปลี่ยน

นอกจากนั้น หากเป็นกรณีการขอซื้อเงินตราต่างประเทศเพื่อชำระหนี้เงินกู้จากต่างประเทศ ต้องปฏิบัติตามประกาศเจ้าพนักงานควบคุมการแลกเปลี่ยนเงิน เรื่อง การกำหนดหลักเกณฑ์ และวิธีปฏิบัติเกี่ยวกับการแลกเปลี่ยนเงิน ฉบับลงวันที่ 1 เมษายน 2534 และฉบับที่ 9 ลงวันที่ 11 มกราคม 2544 โดยกำหนดให้บุคคลใดขอซื้อหรือแลกเปลี่ยนหรือถอนหรือกู้ยืมเงินตราต่างประเทศกับตัวแทนรับอนุญาตเพื่อวัตถุประสงค์ชำระคืนต้นเงินกู้จากต่างประเทศ ตัวแทนรับอนุญาต ต้องเรียกให้บุคคลนั้นยื่นเอกสารหลักฐานตามที่ระบุไว้แต่ละกรณีดังต่อไปนี้

1. หลักฐานที่แสดงถึงรายละเอียดของการกู้ยืมจากต่างประเทศ เช่น สัญญากู้
2. หลักฐานการนำเงินกู้จากต่างประเทศนั้นเข้ามาในประเทศ

2.5.1.2.3. พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542

หากพิจารณาถึง การกระทำอันเป็นการนำเครื่องหรือระบบโอนเงินทางอิเล็กทรอนิกส์มาใช้เป็นเครื่องมือในการฟอกเงิน ซึ่งความผิดดังกล่าวจึงควรต้องพิจารณาตามบทบัญญัติแห่งพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ได้มีบทบัญญัติที่กำหนดให้ "การปกปิดหรือเปลี่ยนสภาพ ซึ่งเงินหรือทรัพย์สินที่ได้มาจากการกระทำความผิดหรือการได้มาโดยมิชอบด้วยกฎหมายหรือไม่สุจริตในความผิดมูลฐานแห่งพระราชบัญญัติฉบับนี้ ให้กลายเป็นเงินที่ได้มาโดยชอบด้วยกฎหมาย หรือพิสูจน์ไม่ได้ว่าเป็นเงินที่ได้มาจากการกระทำ

ความผิดหรือทุจริต" เป็นความผิดฐานฟอกเงิน ประกอบกับปัจจุบันได้มีการใช้กระบวนการโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการฟอกเงิน ดังนั้นการบังคับใช้กฎหมายกับกรณีดังกล่าวจึงควรต้องศึกษาถึงพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พศ. 2542 โดยมีข้อควรพิจารณาดังนี้

ตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 จะมีองค์ประกอบความผิดดังนี้

1. การเปลี่ยนสภาพ หรือปกปิดเงินหรือทรัพย์สินที่ได้มาจากการกระทำความผิด หรือได้มาโดยมิชอบด้วยกฎหมายหรือไม่สุจริตให้กลายเป็นเงินที่ได้มาโดยชอบด้วยกฎหมาย หรือพิสูจน์ไม่ได้ว่าเป็นเงินที่ได้มาจากการกระทำความผิดหรือทุจริต
2. เงินหรือทรัพย์สินดังกล่าวต้องเป็นเงินหรือทรัพย์สินที่ได้มาจากความผิดเฉพาะที่กำหนดไว้ในพระราชบัญญัติฉบับดังกล่าว ซึ่งกำหนดไว้ในความผิด 7 มูลฐาน กล่าวคือ
   (1) ความผิดเกี่ยวกับยาเสพติดตามกฎหมายว่าด้วยการป้องกันและปราบปรามยาเสพติด หรือกฎหมายว่าด้วยมาตรการในการปราบปรามผู้กระทำความผิดเกี่ยวกับยาเสพติด
   (2) ความผิดเกี่ยวกับเพศตามประมวลกฎหมายอาญา
   (3) ความผิดเกี่ยวกับการฉ้อโกงประชาชน ตามประมวลกฎหมายอาญา หรือความผิดตามกฎหมายว่าด้วยการกู้ยืมเงินซึ่งเป็นลักษณะของการฉ้อโกงประชาชน
   (4) ความผิดเกี่ยวกับการยักยอก ฉ้อโกง หรือประทุษร้ายต่อทรัพย์หรือกระทำโดยทุจริต ตามกฎหมายว่าด้วยการธนาคารพาณิชย์ กฎหมายว่าด้วยการประกอบธุรกิจเงินทุน ธุรกิจหลักทรัพย์และธุรกิจเครดิตฟองซิเอร์ หรือกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ ซึ่งกระทำโดยกรรมการผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบหรือมีประโยชน์เกี่ยวข้องกับในการดำเนินงานของสถาบันการเงินนั้น
   (5) ความผิดต่อตำแหน่งข้าราชการหรือความผิดต่อตำแหน่งหน้าที่ในการยุติธรรมตามประมวลกฎหมายอาญา ความผิดตามกฎหมายว่าด้วยความผิดของพนักงานในองค์การ หรือ

หน่วยงานของรัฐ หรือความผิดต่อตำแหน่งหน้าที่หรือทุจริตต่อหน้าที่ตามกฎหมายอื่น

(6) ความผิดเกี่ยวกับการกรรโชก หรือเอาทรัพย์ที่กระทำโดยอำนาจอั้งยี่หรือซ่องโจรตามประมวลกฎหมายอาญา

(7) ความผิดเกี่ยวกับการลักลอบหนีศุลกากรตามกฎหมายว่าด้วยศุลกากร

3. การเปลี่ยนสภาพหรือการปกปิดเงินที่ได้มาจากการกระทำความผิดมูลฐานข้างต้น โดยวิธีการลักษณะใดๆ

หากพิจารณาถึง มาตรการทางกฎหมายตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 ได้กำหนดมาตรการทางกฎหมายที่บังคับใช้กับการกระทำความผิดฐานฟอกเงินซึ่งรวมถึงการฟอกเงินในการโอนเงินทางอิเล็กทรอนิกส์ด้วย โดยมีสาระสำคัญดังนี้

1. การกำหนดให้สถาบันทางการเงิน มีหน้าที่ต้องรายงานการทำธุรกรรมทางการเงินอย่างเป็นระบบ โดยธุรกรรมที่ต้องรายงานต่อสำนักงานคณะกรรมป้องกันและปราบปรามการฟอกเงินได้แก่ หากปรากฏหลักฐานที่เชื่อได้ว่าทรัพย์สินในธุรกรรมนั้นเกี่ยวข้องกับการกระทำความผิดจะต้องเสนอรายงานต่อผู้บังคับบัญชา ในธุรกรรมซึ่ง

(1) มีเหตุอันควรสงสัยว่าธุรกรรมเกี่ยวข้องหรืออาจเกี่ยวข้องกับการกระทำความผิดฐานฟอกเงิน

(2) มีพยานหลักฐานเป็นที่เชื่อได้ว่าธุรกรรมเกี่ยวข้องหรืออาจเกี่ยวข้องกับการกระทำความผิดฐานฟอกเงิน

2. การกำหนดมาตรการริบทรัพย์สินในการใช้บังคับกับทรัพย์สินที่ได้มาจากการฟอกเงิน มาตรการริบทรัพย์สินตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ได้กำหนดลักษณะพิเศษนอกเหนือจากการริบทรัพย์สินที่กำหนดไว้ในประมวลกฎหมายอาญา โดยการริบทรัพย์สินตามประมวลกฎหมายอาญาได้กำหนดให้ริบทรัพย์สินได้เฉพาะทรัพย์สินที่เป็นทรัพย์สินที่ได้ใช้หรือได้มาจากการกระทำความผิด ซึ่งมุ่งบังคับใช้เฉพาะฐานความผิดตามประมวลกฎหมายอาญาโดยเฉพาะเจาะจง ซึ่งการริบทรัพย์สินตามประมวลกฎหมายอาญาจึงไม่อาจใช้บังคับกับการริบทรัพย์สินที่เป็นความผิดฐานฟอกเงินได้ ซึ่งมาตรการริบทรัพย์สินตามความผิดฐานฟอกเงินแห่งพระราชบัญญัติฉบับนี้มีสาระสำคัญคือ

(1) ธุรกรรมที่มีเหตุอันควรเชื่อได้ว่าทรัพย์สินที่โอนในธุรกรรมนั้นเป็นทรัพย์สินที่เกี่ยวกับการกระทำความผิด

(2) คณะกรรมการเลขาธิการหรือเลขาธิการป.ป.ง.มีอำนาจสั่งยึด-อายัดทรัพย์สินดังกล่าวไว้ชั่วคราวไม่เกิน 90 วัน ซึ่งผู้ที่มีส่วนได้เสียในทรัพย์สินนั้นมีสิทธิยื่นคำร้อง และแสดงหลักฐานว่าเงินหรือทรัพย์สินนั้นมิใช่ทรัพย์สินที่ได้มาจากการกระทำความผิดเพื่อให้คณะกรรมการธุรกรรมพิจารณา และมีอำนาจสั่งเพิกถอนการยึด-อายัดกรณีดังกล่าวได้

(3) ระหว่างการยึด-อายัดทรัพย์สินดังกล่าว หากมีเหตุอันควรเชื่อได้ว่าจะมีการโอน ยักย้าย จำหน่ายทรัพย์สินดังกล่าว โดยให้เลขาธิการสำนักงานป้องกันและปราบปรามการฟอกเงินส่งเรื่องให้อัยการร้องต่อศาลแพ่งเพื่อร้องขอคำสั่งยึดทรัพย์สินดังกล่าวให้ตกเป็นของแผ่นดิน ซึ่งศาลแพ่งเป็นต้องพิจารณาคำขอเป็นการด่วนและเป็นผู้ไต่สวนคำร้องของคู่กรณีดังกล่าว และหากปรากฏหลักฐานเป็นที่เชื่อได้ว่าทรัพย์สินนั้นเกี่ยวข้องกับการกระทำความผิดศาลมีคำสั่งให้ทรัพย์สินนั้นตกเป็นของแผ่นดิน

3. การกำหนดหน่วยงานพิเศษในการบังคับใช้กฎหมาย กับการกระทำความผิดลักษณะฟอกเงินดังกล่าว โดยพระราชบัญญัติฉบับนี้กำหนดให้สำนักงานป้องกันและปราบปรามการฟอกเงินเป็นหน่วยงานรับรายงานการทำธุรกรรม เก็บรวบรวม ติดตาม ตรวจสอบ ศึกษา และวิเคราะห์รายงานและข้อมูลที่เกี่ยวกับธุรกรรม และเก็บรวบรวมพยานหลักฐานที่เกี่ยวกับการกระทำความผิดตามบทบัญญัตินี้ เพื่อให้การบังคับใช้กฎหมายฟอกเงินกับการกระทำความผิดดังกล่าวอยู่ภายใต้อำนาจหน้าที่ของเจ้าพนักงานที่เป็นผู้ที่มีความรู้ความชำนาญและมีความสามารถพิเศษเกี่ยวกับการกระทำความผิดตามมาตรานี้

จากการศึกษาข้างต้น จะเห็นได้ว่าพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ยังมีข้อจำกัดในการบังคับใช้กฎหมายฟอกเงินกับการกระทำที่อาชญากรรมคอมพิวเตอร์ ในการโอนเงินทางอิเล็กทรอนิกส์ในหลายประการกล่าวคือ

1. ข้อจำกัดในที่มาของเงิน หรือทรัพย์สินที่ได้มาจากการกระทำความผิดซึ่งกำหนดไว้เพียงความผิดใน 7 มูลฐานดังที่กล่าวข้างต้น
2. ข้อจำกัดเฉพาะการโอนทางอิเล็กทรอนิกส์ เพื่อแปรสภาพหรือปกปิดที่มาของเงินหรือทรัพย์สินดังกล่าวว่าเป็นเงินหรือทรัพย์สินที่ได้มาจากการกระทำความผิดหรือทุจริต

ดังนั้นหากการกระทำในลักษณะอื่นๆ ในการโอนเงินทางอิเล็กทรอนิกส์ที่อยู่นอกเหนือจากข้อจำกัดดังกล่าวย่อมไม่เป็นความผิดฐานฟอกเงิน และไม่อยู่ในมาตรการทางกฎหมายที่บังคับใช้กับการกระทำความผิดฐานฟอกเงินแห่งพระราชบัญญัติฉบับนี้ที่กล่าวมาแล้วข้างต้น และนอกเหนือจากกฎหมายฟอกเงินแล้วประเทศไทยยังไม่มีกฎหมายฉบับใดที่บังคับใช้กับอาชญากรรมคอมพิวเตอร์ในการโอนเงินทางอิเล็กทรอนิกส์ได้

2.5.2 ปัญหาและอุปสรรคด้านพยานหลักฐานทางหรือพยานหลักฐานทางคอมพิวเตอร์กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

เนื่องจากการกระทำความผิดโดยตรงต่อเครื่อง หรือระบบอิเล็กทรอนิกส์เพื่อทำการโอนเงินทางอิเล็กทรอนิกส์ หรือการใช้ระบบการโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิด แต่หากพิจารณาถึงปัญหาด้านพยานหลักฐานที่บังคับใช้กับการดำเนินคดีทางอาญาตามประมวลวิธีพิจารณาความอาญาไทย จะเห็นได้ว่า ประมวลวิธีพิจารณาความอาญา มาตรา 226 ได้กำหนดถึง กฎหมายกำหนดให้พยานหลักฐานที่รับฟังได้โดยกำหนดให้พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือเป็นผู้บริสุทธิ์ให้สามารถใช้อ้างเป็นพยานหลักฐานได้ แต่ต้องมิใช่พยานหลักฐานที่เกิดจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น และให้สืบพยานตามบทบัญญัติว่าด้วยการสืบพยาน

หากพิจารณาถึง พยานหลักฐานแห่งการกระทำความผิดในการโอนเงินทางอิเล็กทรอนิกส์ซึ่งถือเป็นพยานหลักฐานทางคอมพิวเตอร์อย่างหนึ่ง จากการศึกษาพบว่าประมวลกฎหมายวิธีพิจารณาความอาญาของไทย ยังไม่มีบทบัญญัติรับรองการรับฟังพยานหลักฐานทางคอมพิวเตอร์ หรือพยานหลักฐานทางอิเล็กทรอนิกส์ดังกล่าวไว้แต่อย่างใด ดังนั้นจึงมีประเด็นปัญหาที่ควรพิจารณาหลายประการ ดังนี้

1. <u>พยานหลักฐานที่ได้จากระบบโอนเงินทางอิเล็กทรอนิกส์ถือเป็นพยานวัตถุหรือพยานเอกสาร</u>

พยานหลักฐานแห่งการกระทำความผิดในการโอนเงินทางอิเล็กทรอนิกส์ถือเป็นพยานหลักฐานทางคอมพิวเตอร์ ซึ่งหากพิจารณาพยานหลักฐานทางคอมพิวเตอร์แล้วจะจัดว่าเป็นพยานวัตถุที่หมายถึง วัตถุที่เป็นสิ่งของที่คู่ความอ้างเป็นพยาน พยานวัตถุบางประเภทอาจอยู่ในรูปของพยานเอกสาร เช่น ภาพถ่าย หรือภาพวาด และพยานเอกสารที่หมายถึงข้อความ ตัวหนังสือ ลายลักษณ์อักษร รูปรอยใด

ของพยานเอกสาร เช่น ภาพถ่าย หรือภาพวาด และพยานเอกสารที่หมายถึงข้อความ ตัวหนังสือ ลายลักษณ์อักษร รูปรอยใด

ซึ่งจากการพิจารณาถึงพยานหลักฐานที่ได้จากระบบอิเล็กทรอนิกส์ หรือคอมพิวเตอร์จะเห็นได้ว่า แม้ว่าคอมพิวเตอร์จัดเป็นวัตถุอย่างหนึ่งแต่พยานหลักฐานที่ได้จากคอมพิวเตอร์เป็นหลักฐานที่แสดงถึงสื่อทางภาษา ประกอบกับพยานเอกสารไม่จำเป็นต้องอยู่ในกระดาษเสมอไป อาจอยู่ในฝ้า แผ่นไม้ แผ่นศิลา กระจก ก็ได้ ด้วยเหตุนี้ ข้อความที่บันทึกอยู่ในเครื่องคอมพิวเตอร์เมื่อพิมพ์ออกมาแล้วจะสื่อความหมายทางภาษาอย่างหนึ่งอย่างใด จึงจัดได้ว่าเป็นพยานเอกสาร

2. <u>ซึ่งหากพิจารณาว่าพยานหลักฐานทางคอมพิวเตอร์เป็นพยานเอกสารแล้ว พยานหลักฐานทางคอมพิวเตอร์ที่เป็น Printout หรือ Disk จัดเป็นต้นฉบับเอกสารที่สามารถนำอ้างตามประมวลกฎหมายวิธีพิจารณาความอาญาได้หรือไม่</u>

กรณีดังกล่าวต้องพิจารณาจากการอ้างพยานหลักฐาน ตามประมวลวิธีพิจารณาทางอาญา มาตรา 238 ได้กำหนดให้ "พยานเอกสารต้องอ้างต้นฉบับเอกสารเท่านั้น ถ้าหาต้นฉบับไม่ได้ให้สำเนาถูกต้อง หรือใช้พยานบุคคลที่รู้เห็นเอกสารดังกล่าว" ซึ่งพยานหลักฐานทางคอมพิวเตอร์ต้องมีการแปรสภาพออกมาให้อยู่ในรูปของ Printout หรือ Disk หรือสื่อบันทึกในรูปแบบอื่นจึงต้องพิจารณาว่าจัดเป็นต้นฉบับเอกสารหรือไม่ และหากไม่จัดเป็นต้นฉบับเอกสารแล้ว Printout หรือ Disk ดังกล่าว จัดเป็นพยานหลักฐานที่เป็นไปตามข้อยกเว้นกรณีหาต้นฉบับไม่ได้หรือไม่ หรือเป็นพยานหลักฐานที่ต้องอ้างพยานบุคคลในการรับรองพยานหลักฐานดังกล่าว

ซึ่งจากการพิจารณาแล้วเห็นว่า Printout หรือ Disk มิใช่พยานเอกสารที่หาต้นฉบับไม่ได้ด้วยเป็นเอกสารที่พิมพ์ออกมาจากเครื่องคอมพิวเตอร์โดยตรง ดังนั้นจึงเห็นว่า Printout หรือ Disk ไม่เข้าข้อยกเว้นแห่งกรณีการใช้สำเนารับรองถูกต้องแทนพยานเอกสารที่หาต้นฉบับไม่ได้ การตีความต่อไปในพยานเอกสารดังกล่าวว่า Printout หรือ Disk นั้นเป็นต้นฉบับเอกสารหรือไม่ ซึ่งหากคู่ความพิจารณาและคัดค้านว่าพยานเอกสารดังกล่าวไม่ใช่ต้นฉบับ ศาลอาจไม่รับฟังพยานเอกสารดังกล่าวได้ และกรณีนี้ยังไม่มีคำพิพากษาฎีกาตีความในเรื่องดังกล่าวไว้

3. การพิสูจน์ความถูกต้องแท้จริงของพยานหลักฐานทางคอมพิวเตอร์

โดยปกติตามประมวลกฎหมายวิธีพิจารณาทางอาญาถือว่า พยานเอกสารจัดเป็นพยานหลักฐานที่ถูกต้องแท้จริง และให้นำอ้างต้นฉบับเอกสารดังกล่าว แต่หากพิจารณาถึงพยานหลักฐานทางคอมพิวเตอร์แล้ว จะตีความว่าพยานหลักฐานดังกล่าวมีความถูกต้องแท้จริงมากน้อยเพียงใด ซึ่งโดยปกติการนำสืบพยานเอกสารต้องพิสูจน์ความถูกต้องแท้จริงของพยานหลักฐานดังกล่าวเฉพาะกรณีที่มีผู้คัดค้านเท่านั้น ตามประมวลกฎหมายวิธีพิจารณาความอาญาได้กำหนดไว้ในมาตรา 125 กล่าวคือ คู่ความมีสิทธิคัดค้านพยานเอกสารนั้นใน 3 กรณีกล่าวคือ

- เอกสารไม่มีต้นฉบับ
- ต้นฉบับเอกสารปลอมทั้งหมดหรือแต่บางส่วน
- สำเนาเอกสารไม่ถูกต้องกับต้นฉบับ

หากพิจารณาจากกรณีที่คู่ความมีสิทธิคัดค้านพยานเอกสารดังกล่าวได้ จะเห็นได้ว่าพยานหลักฐานทางคอมพิวเตอร์ที่เป็น Printout หรือ Disk ซึ่งอาจถูกคัดค้านได้ในประเด็นเอกสารดังกล่าวไม่ใช่ต้นฉบับ หรือผู้คัดค้านอาจมีความสงสัยว่าเอกสารนั้นปลอมหรือไม่ถูกต้อง และกรณีนี้ผู้คัดค้านจึงต้องขอดูต้นฉบับ ดังนั้นการดำเนินคดีที่เกี่ยวข้องกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งเป็นประเด็นสำคัญว่าคดีดังกล่าวจะต้องมีความเกี่ยวข้องกับพยานหลักฐานทางคอมพิวเตอร์อย่างแน่นอน ดังนั้นจึงเป็นประเด็นว่าพยานหลักฐานทางคอมพิวเตอร์ที่มีผู้นำอ้างเอกสารดังกล่าวในคดีแล้ว จะพิสูจน์ถึงความถูกต้องของพยานหลักฐานดังกล่าวได้อย่างไร

2.6 ตัวอย่างอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

2.6.1 สถิติอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ประเทศสหรัฐอเมริกา

คดีที่ขึ้นสู่ศาล ณ ประเทศสหรัฐอเมริกา โดยจัดทำสถิติแยกในแต่ละลักษณะของการกระทำความผิด ซึ่งถือเป็นอาชญากรรมทางด้านการเงินการธนาคาร ตั้งแต่วันที่ 1 เมษายน 2539 จนถึง 31 ธันวาคม 2543

Exhibit 4[38]

Frequency Distribution of SAR Filings by Characterization
of Suspicious Activity in Descending Order
For the Period April 1, 1996 through December 31, 2000

Rank	State/Territory	Filings (Overall)	Percentage [3] (Overall)
1	BSA/Structuring/Money Laundering	255,653	46%
2	Check Fraud	71,622	13%
3	Other	39,977	7.2%
4	Counterfeit Check	28,908	5.2%
5	Defalcation/Embezzlement	24,998	4.5%
6	Credit Card Fraud	24,054	4.3%
7	Check Kiting	21,306	3.85%
8	Unknown/Blank	20,963	3.8%
9	Mortgage Loan Fraud	11,703	2.1%
10	False Statement	11,416	2.05%
11	Consumer Loan Fraud	11,362	2.05%
12	Mysterious Disappearance	8,872	1.6%
13	Misuse of Position or Self Dealing	8,345	1.5%
14	Commercial Loan Fraud	4,819	Less than 1%
15	Debit Card Fraud	3,352	Less than 1%
16	Wire Transfer Fraud	3,121	Less than 1%
17	Counterfeit Credit/Debit Card	1,969	Less than 1%
18	Counterfeit Instrument (Other)	1,564	Less than 1%
19	Bribery/Gratuity	544	Less than 1%
20	Computer Intrusion [4]	65	Less than 1%

[3] All percentages are approximate.
[4] Separate box on form for this violation was added in June 2000 TD F 90-22.47, and statistics date from that period.

---

[38] The SAR Activity Review, Trends Tips & Issues (Issues2).(Financial Crimes Enforcement Network : Bank Secrecy Act Advisory Group),p.9.

คดีที่ขึ้นสู่ศาล ณ ประเทศสหรัฐอเมริกา โดยแบ่งออกเป็นความผิดในแต่ละลักษณะของการกระทำความผิดซึ่งถือได้ว่าเป็นอาชญากรรมทางการเงินการธนาคาร โดยจัดทำเป็นสถิติของอาชญากรรมที่เกิดขึ้นในแต่ละปี ตั้งแต่วันที่ 1 เมษายน 2539 จนถึง 31 ธันวาคม 2543

Exhibit 5[39]

Frequency Distribution of SAR Filings
by Characterization of Suspicious Activity
For the Period April 1, 1996 through December 31, 2000

Violation	1996	1997	1998	1999	2000
BSA/Structuring/Money Laundering	20,565	35,949	47,509	61,007	90,623
Bribery/Gratuity	91	109	93	101	150
Check Fraud	8,639	13,274	13,832	16,239	19,638
Check Kiting	2,747	4,298	4,037	4,061	6,163
Commercial Loan Fraud	554	960	905	1,080	1,320
Computer Intrusion	0	0	0	0	65 5
Consumer Loan Fraud	1,148	2,048	2,185	2,549	3,432
Counterfeit Check	2,317	4,244	5,918	7,396	9,033
Counterfeit Credit/Debit Card	385	387	182	351	664
Counterfeit Instrument (Other)	212	292	265	321	474
Credit Card Fraud	3,375	5,083	4,383	4,938	6,275
Debit Card Fraud	245	610	566	721	1,210
Defalcation/Embezzlement	3,136	5,306	5,260	5,179	6,117
False Statement	1,807	2,204	1,978	2,376	3,051
Misuse of Position or Self Dealing	914	1,537	1,645	2,063	2,186
Mortgage Loan Fraud	1,265	1,719	2,268	2,936	3,515
Mysterious Disappearance	1,168	1,767	1,855	1,857	2,225
Wire Transfer Fraud	284	499	594	772	972
Other	4,600	6,777	8,696	8,755	11,149
Unknown/Blank	1,652	2,317	2,728	7,295	6,971

5 Separate box on the form for this violation was added in June 2000 TD F 90-22.47, and statistics date from that period.

บทนิยามศัพท์

- การฟอกเงินผ่านระบบการเงินธนาคาร Bank Secrecy Act (BSA/Structuring/Money Laundering)
- การกระทำที่มีการให้ผลประโยชน์ หรือรางวัล (Bribery/Gratuity)
- การฉ้อโกงเช็คหรือตราสาร (Check Fraud)
- การสั่งจ่ายเช็คไม่มีเงิน (Check Kiting)
- การฉ้อโกงหนี้เงินกู้ทางพาณิชย์ (Commercial Loan Fraud)

---

[39] The SAR Activity Review. Trends Tips & Issues (Issues2).(Financial Crimes Enforcement Network : Bank Secrecy Act Advisory Group), p.10.

- การเข้าถึงเครื่องคอมพิวเตอร์ (Computer Intrusion)
- การฉ้อโกงเงินกู้ (Consumer Loan Fraud)
- การปลอมแปลงเช็ค (Counterfeit Check)
- การปลอมบัตรเครดิตและบัตรเดบิต (Counterfeit Credit/Debit Card)
- การปลอมคำสั่งทางการเงินหรือเครื่องมือในการชำระหนี้ต่างๆ (Counterfeit Instrument or Other)
- การฉ้อโกงบัตรเครดิต (Credit Card Fraud)
- การฉ้อโกงบัตรเดบิต (Debit Card Fraud)
- การยักยอกเงินราชการหรือเงินในระบบการเงินการธนาคาร(Defalcation/Embezzlement)
- การแจ้งข้อความอันเป็นเท็จหรือไม่ตรงกับความจริง (False Statement)
- การใช้ตำแหน่งอำนาจหน้าที่เพื่อกระทำการอันมิชอบหรือผิดกฎหมาย (Misuse of Position or Self Dealing)
- การฉ้อโกงหนี้เงินกู้จำนอง (Mortgage Loan Fraud)
- การทำให้ข้อมูลสำคัญสูญหาย (Mysterious Disappearance)
- การฉ้อโกงผ่านระบบการโอนทางโทรเลข โทรศัพท์ หรือเทคโนโลยีสารสนเทศ(Wire Transfer Fraud)
- การกระทำความผิดต่อระบบการเงินการธนาคารในลักษณะอื่นๆ (Other)
- การประกอบกิจการธนาคารที่ไม่ได้รับอนุญาต (Unknown/Blank)

2.6.2 สถิติอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในประเทศไทย[40]

แบบรายการข้อมูลสถิติอาชญากรรมเกี่ยวกับบัตรเครดิต

ปี พ.ศ.	จำนวนคดีทั้งสิ้น (ราย)	จำนวนคดีที่มีการจับกุม (ราย)	จำนวนผู้ต้องหา (ราย)	มูลค่าความเสียหาย (บาท)
พ.ศ. 2545	20	11	13	5,822,708.00.-
พ.ศ. 2544	29	21	40	10,984,911.00.-
พ.ศ. 2543	40	24	38	8,529,421.69.-
พ.ศ. 2542	41	19	25	162,356.82.-
พ.ศ. 2541	61	31	44	13,218,719.27.-
พ.ศ. 2540	70	44	52	12,396,043.18.-
พ.ศ. 2539	44	20	27	19,191,312.83.-
พ.ศ. 2538	63	42	68	16,991,363.71.-
พ.ศ. 2537	44	31	39	1,355,954.03.-
พ.ศ. 2536	43	24	31	8,669,236.00.-

สถิติคดีค้าเงินเถื่อน FOREX

งาน 2 กองกำกับการ 2 กองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ

ปี พ.ศ.	จำนวนคดีที่เกิด (ราย)	จำนวนความเสียหาย (บาท)
2544	7	5,123,333.00.-
2545	2	843,876.34.-
2546	1	1,100,000.00.-

[40] "รายงานสถิติคดีเกี่ยวกับบัตรเครดิต และความผิดค้าเงินเถื่อน", สำนักงานสืบสวนสอบสวนคดีเศรษฐกิจ , (ม.ป.ท.),(ม.ป.ป.),2545.

บทที่ 3

มาตรการกฎหมายต่างประเทศที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

หากพิจารณาถึง มาตรการทางกฎหมายต่างประเทศที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในระบบโอนเงินทางอิเล็กทรอนิกส์ เพื่อวิเคราะห์แนวทางทางด้านกฎหมายที่เหมาะสมในการบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ได้อย่างเหมาะสม และสามารถรักษาเสถียรภาพทางด้านการเงินการธนาคารให้น่าเชื่อถือ และถือได้ว่าประเทศไทยมีแนวทางด้านกฎหมายในการคุ้มครองระบบการเงินการธนาคารที่ได้รับการยอมรับทั่วไป โดยกฎหมายในต่างประเทศที่เป็นแนวทางสำคัญในการกำหนดมาตรการทางกฎหมาย เพื่อบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในปัจจุบัน ไม่ว่าจะเป็นมาตรการกฎหมายของประเทศสหรัฐอเมริกา (United State) ประเทศสหราชอาณาจักร (United Kingdom) สหภาพยุโรป (European Union) องค์การสหประชาชาติ (United Nation) ธนาคารกลางระหว่างประเทศ (Bank for International Settlement) หรือโครงการความร่วมมือระหว่างประเทศในการควบคุมและบังคับใช้กับอาชญากรรมทางการเงินการธนาคาร (Financial Action Task Force)

ซึ่ง แนวทางกฎหมายในต่างประเทศที่บังคับใช้กับกรณีดังกล่าว อาจแบ่งแยกมาตรการทางกฎหมายที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ได้หลายกรณี กล่าวคือ

1. มาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์
2. มาตรการทางกฎหมายในการกำหนดลักษณะความผิดและบทกำหนดโทษกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์
3. มาตรการทางกฎหมายในการแก้ไขเยียวยาความเสียหายที่เกิดขึ้นจากอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์
4. มาตรการทางกฎหมายในการกำหนดหน่วยงานพิเศษเพื่อบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์
5. มาตรการทางกฎหมายด้านความร่วมมือระหว่างประเทศ

3.1. มาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

3.1.1 ประเทศสหรัฐอเมริกา (United State)

เนื่องจากประเทศสหรัฐอเมริกาได้มีการพัฒนากฎหมายที่บังคับใช้กับการโอนเงินทางอิเล็กทรอนิกส์เรื่อยมา ประกอบกับมีระบบการเงินการธนาคารที่ค่อนข้างซับซ้อน ด้วยเหตุว่ามีการแบ่งแยกการบังคับใช้กฎหมายออกเป็นกฎหมายมลรัฐ และกฎหมายสหพันธรัฐ ด้วยเหตุนี้การโอนเงินทางอิเล็กทรอนิกส์ของธนาคาร หรือสถาบันการเงินต่าง ๆ ในประเทศสหรัฐอเมริกาจึงอยู่ภายใต้การกำกับดูแลและการควบคุมกฎหมายหรือองค์กรต่าง ๆ จากหลายหน่วยงานตามแต่ละอำนาจหน้าที่ที่กฎหมายแต่ละฉบับได้กำหนดขึ้นให้ทำหน้าที่ควบคุมดูแลธุรกรรมทางการเงินการธนาคารภายในมลรัฐหรือรัฐบาลกลาง

การโอนเงินทางอิเล็กทรอนิกส์ภายใต้ระบบการชำระเงิน หรือระบบการหักบัญชีทางอิเล็กทรอนิกส์ของธนาคารหรือสถาบันทางการเงินต่าง ๆ ในการให้บริการทางการเงินการธนาคารของประเทศสหรัฐอเมริกาสามารถแบ่งออกเป็น 3 ระบบใหญ่ๆ ได้ดังนี้

1.ระบบ Clearing House Interbank Payments System หรือ CHIPS เป็นระบบออนไลน์หรือระบบที่เชื่อมโยงเครือข่ายของการโอนเงินและการหักบัญชี ณ เวลาเดียวกัน โดยทำงานแบบ real–time System ซึ่งสมาคมสำนักหักบัญชีแห่งรัฐนิวยอร์คจะทำการหักบัญชีของธนาคารที่มีการโอนเงิน หรือธุรกรรมทางการเงินในแต่ละแห่งผ่านธนาคารกลางแห่งรัฐนิวยอร์ค (Federal Reserve Bank of New York) ทำให้ระบบดังกล่าวสามารถอำนวยความสะดวกในการโอนเงินระหว่างประเทศยกตัวอย่างเช่น การโอนเงินระหว่างเงินสกุลดอลล่าร์กับเงินสกุลยูโรที่มีการแลกเปลี่ยนเงินตราต่างประเทศระหว่างเงินสกุลดอลลาร์กับเงินสกุลยูโร ณ เวลาที่มีการโอนเงินรายนั้นๆ โดยระบบ CHIPS ทำให้การโอนเงินระหว่างประเทศสามารถหักบัญชีระหว่างธนาคารโดยหักบัญชีผ่านธนาคารกลางแห่งรัฐนิวยอร์คกับธนาคารในรัฐอื่น ๆ ระหว่างรัฐสามารถกระทำได้อย่างมีประสิทธิภาพ

2. การโอนเงินผ่านระบบ FedWire® ซึ่งเป็นระบบการหักบัญชีรายใหญ่หรือการหักบัญชีระหว่างรัฐที่มีการหักบัญชีผ่านเครือข่าย FEDNET® ซึ่งเป็นเครือข่ายติดต่อสื่อสารแห่งชาติที่เชื่อมโยงการหักบัญชีธนาคารระหว่างธนาคารรัฐบาลกลางของสหรัฐอเมริกากับธนาคาร หรือสถาบันทางการเงินภายในประเทศสหรัฐอเมริกาทั้งหมดในการดำเนินธุรกรรมทางอิเล็กทรอนิกส์

หรือการโอนเงินทางอิเล็กทรอนิกส์ โดยใช้ระบบคอมพิวเตอร์ที่มีการทำงานแบบ Real-time Gross Settlement (RTGS) มาเป็นสื่อกลางในการหักบัญชีของผู้ใช้บริการที่ทำการโอนเงิน หรือดำเนินธุรกรรมทางการเงินระหว่างธนาคารรัฐบาลกลางกับสถาบันทางการเงินการธนาคารของประเทศสหรัฐอเมริกาทั้งหมด

3. ระบบ ACH หรือ Automatic Clearing House เป็นระบบที่รองรับการหักบัญชีระหว่างธนาคารกับธนาคาร หรือระบบการหักบัญชีระหว่างธนาคารกับผู้ใช้บริการ ด้วยเหตุนี้ระบบดังกล่าวจึงเกิดขึ้นสำหรับการรองรับการทำธุรกรรมทางการเงินการธนาคารอิเล็กทรอนิกส์ผ่านทางธนาคารประเภทต่าง ๆ ผ่านระบบการเงินการธนาคารในประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาได้มีการกำหนดบทบัญญัติทางกฎหมายที่บังคับใช้กับการโอนเงินทางอิเล็กทรอนิกส์ ไว้โดยตรง ซึ่งได้บัญญัติไว้ในกฎหมาย 2 ฉบับ กล่าวคือ

1. กฎหมายพาณิชย์ของสหรัฐอเมริกา มาตรา 4A (Uniform Commercial Code Article 4A)

กฎหมายพาณิชย์ของสหรัฐอเมริกา มาตรา 4A ได้กล่าวถึงรายละเอียดของคำสั่งโอนเงิน ขอบเขตอำนาจหน้าที่ และความรับผิดชอบของแต่ละฝ่ายที่เกี่ยวข้องกับคำสั่งโอนเงิน โดยให้มีผลในการเคลื่อนย้ายเงินจากบัญชีหนึ่งไปยังอีกบัญชีหนึ่งโดยมีผู้ที่เกี่ยวข้อง คือ ผู้ส่ง (Sender) ธนาคารผู้โอนเงิน (Originator's Bank) ธนาคารผู้รับโอน (Receiving Bank) ธนาคารผู้รับประโยชน์ (Beneficiary's Bank) และผู้รับประโยชน์ (Beneficiary) ซึ่งบทบัญญัติฉบับนี้ ได้กำหนดความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ให้มีความผูกพันกันในลักษณะความสัมพันธ์ระหว่างลูกหนี้กับเจ้าหนี้ และความรับผิดชอบของแต่ละฝ่ายที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ หากแต่มิได้มีบทบัญญัติในการบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ไว้

2. พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 (Electronic Fund Transfer Act)

พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ (Electronic Funds Transfer Act, 1978) เป็นบทบัญญัติที่ใช้บังคับกับการโอนเงินทางอิเล็กทรอนิกส์ของผู้ใช้บริการรายย่อยโดยเฉพาะ ไม่ว่าจะเป็นการฝากถอนเงินทางอิเล็กทรอนิกส์ผ่านบัญชีของผู้ใช้บริการ การฝาก ถอน

หรือโอนเงินผ่านเครื่องฝากและถอนเงินอัตโนมัติ เช่น การโอนเงิน ณ จุดขาย การหักบัญชีเพื่อชำระค่าโทรศัพท์ การโอนเงินทางธนาคารอิเล็กทรอนิกส์ผ่านคอมพิวเตอร์ที่บ้าน หรือระบบอินเทอร์เน็ต โดยบทบัญญัติดังกล่าวจึงเป็นบรรทัดฐานในการโอนเงินทางอิเล็กทรอนิกส์ รวมไปถึงการกำหนดความรับผิดทางอาญาไว้ในบางกรณี

หากพิจารณาถึง อาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ซึ่งลักษณะความผิดของอาชญากรรมดังกล่าวมีการขยายตัว และมีรูปแบบของแต่ละลักษณะความผิดที่แตกต่างกัน และสามารถสร้างความเสียหายต่อระบบการเงินการธนาคารทั้งในระดับภาครัฐบาลและภาคเอกชน ไม่ว่าจะเป็นความเสียหายต่อระบบการเงินการธนาคาร ระบบเศรษฐกิจ และเสถียรภาพทางการเงินการธนาคารของประเทศสหรัฐอเมริกาได้มากขึ้นตามลำดับ ประกอบกับกฎหมายทั้งสองฉบับดังกล่าวยังมิอาจใช้บังคับได้ครอบคลุมกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ได้ในหลายฐานความผิด

ด้วยเหตุนี้ ประเทศสหรัฐอเมริกาจึงได้มีการออกบทบัญญัติทางกฎหมายอื่นๆ เพื่อการบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นการควบคุมและกำกับดูแลการโอนเงินทางอิเล็กทรอนิกส์ของประเทศนอกเหนือจากพระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ.1978 ซึ่งได้กำหนดในความรับผิดทางอาญาเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ไว้

หากพิจารณาถึง มาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ นั้นได้มีการบัญญัติไว้ในพระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ.1978 (Electronic Fund Transfer Act : EFTA)[1] พระราชบัญญัติความลับทางธนาคาร (Bank Secrecy Act)[2] และพระราชบัญญัติต่อต้านการฟอก

---

[1] United State Code, (Title 15 : Commerce and Trade, Chapter 41 : Consumer Credit Protection, Subchapter VI : Electronic Fund Transfers, section 1693-1693r). [online] Available from : http://caselaw.lp.findlaw.com.

[2] United State Code, (Title 12 : Money and Finance, Chapter 53 Monetary Transaction, in particular, Subchapter II – Records and Reports on money Instruments Transaction and Subchapter III – Money Laundering and Related Financial Crimes, section 5311-5355). [online] Available from : http://caselaw.lp.findlaw.com.

เงินระหว่างประเทศและการต่อต้านการก่อการร้าย ค.ศ. 2001 (The International Money Laundering Abatement and Anti-Terrorist Financial Act of 2001 : IMLA)[3] โดยมาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ของกฎหมายแต่ละฉบับ มีสาระสำคัญดังนี้

3.1.1.1 พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 (Electronic Fund Transfer Act, 1978)

พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 ถือได้ว่าเป็นกฎเกณฑ์ทางกฎหมายในการบังคับใช้กับการโอนเงินทางอิเล็กทรอนิกส์ของประเทศสหรัฐอเมริกาไว้โดยเฉพาะ โดยสภานิติบัญญัติแห่งประเทศสหรัฐอเมริกาอาศัยอำนาจแห่งมาตรา 904 แห่งประมวลกฎหมายสหรัฐอเมริกาในการบัญญัติกฎหมายฉบับนี้ไว้ในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 15 ว่าด้วยการพาณิชย์และการค้า ลักษณะที่ 41 การคุ้มครองเครดิตของผู้ใช้บริการทางการเงิน หมวดที่ 6 ว่าด้วยการโอนเงินทางอิเล็กทรอนิกส์ ตั้งแต่มาตรา 1693-1693r เพื่อเป็นกฎหมายที่บังคับใช้กับการโอนเงินทางอิเล็กทรอนิกส์ของประเทศสหรัฐอเมริกาโดยเฉพาะ

พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์นี้ มีวัตถุประสงค์สำคัญในการกำหนดโครงสร้างพื้นฐานสำหรับปกป้อง และคุ้มครองผู้ใช้บริการรายย่อยในการโอนเงินทางอิเล็กทรอนิกส์ กำหนดขอบเขตของสิทธิ หน้าที่ ความรับผิดของผู้ที่เกี่ยวข้องทั้งหมดที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์หลักในการมุ่งปกป้อง คุ้มครองสิทธิและหน้าที่ของผู้ใช้บริการโอนเงินทางอิเล็กทรอนิกส์ กำหนดกฎและระเบียบแห่งการโอนเงินทางอิเล็กทรอนิกส์ รวมถึงมาตรการต่างๆ ในการบังคับใช้อาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ของธนาคาร หรือสถาบันทางการเงินในประเทศสหรัฐอเมริกา ไม่ว่าจะเป็นมาตรการทางกฎหมายในการป้องกัน มาตรการทางกฎหมายในการกำหนดลักษณะความผิด มาตรการทางกฎหมายในการกำหนดบทลงโทษ และมาตรการทางกฎหมายในการสืบสวนสอบสวนและติดตามผู้กระทำความผิด เพื่อให้การโอนเงินทางอิเล็กทรอนิกส์เป็นไปในแนวทางที่เหมาะสม

---

[3] USA PATROIT ACT, 2001,(Title III : International Money Laundering Abatement and Anti-terrorist Financing.)[online] Available from : http://www4.law.cornell.edu/uscode/html.

ทั้งนี้ มาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์มีสาระสำคัญดังนี้

3.1.1.1.1 การโอนเงินทางอิเล็กทรอนิกส์ต้องอยู่ภายใต้การกำกับ ดูแล และการควบคุมคณะกรรมการกลางแห่งธนาคารรัฐบาลกลาง

พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์นี้ได้กำหนดให้ การโอนทางอิเล็กทรอนิกส์ ภายใต้ระบบการเงินการธนาคารแห่งประเทศสหรัฐอเมริกาต้องปฏิบัติตามกฎ กฎเกณฑ์ ระเบียบ อนุมาตราต่างๆ หรือระเบียบปฏิบัติสำหรับหน่วยงานอื่น ๆ นอกเหนือจากธนาคารหรือสถาบันการเงินที่กำหนดขึ้นโดยคณะกรรมการกลาง ซึ่งคณะกรรมการกลางในที่นี้หมายถึง คณะกรรมการกลางแห่งธนาคารรัฐบาลกลางสหรัฐอเมริกา (Board of Governors of the Federal Reserve System) ซึ่งคณะกรรมการกลางดังกล่าวมีอำนาจหน้าที่ในการออกกฎ ระเบียบ อนุมาตรา หรือระเบียบปฏิบัติต่าง ๆ ถือเป็นเงื่อนไขของการโอนเงินทางอิเล็กทรอนิกส์ เพื่อเป็นการกำหนดสิทธิ หน้าที่ และความรับผิดของผู้ใช้บริการ สถาบันทางการเงินหรือธนาคาร หรือผู้ที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ทั้งหมด หรือควบคุมธุรกรรมทางการเงินการธนาคารของธนาคารหรือสถาบันทางการเงินต่าง ๆ ในประเทศสหรัฐอเมริกาให้เป็นไปอย่างเรียบร้อย

ซึ่งกฎ ระเบียบ อนุมาตราต่างๆ ที่ควบคุม กำกับ ดูแลการโอนเงินทางอิเล็กทรอนิกส์ที่อยู่ภายใต้อำนาจ หน้าที่ของคณะกรรมการกลางดังกล่าว มีรายละเอียดดังต่อไปนี้

1. การพิจารณาและการอนุญาตในการให้บริการทางการเงินการธนาคาร
2. การควบคุมการให้บริการการโอนเงินทางอิเล็กทรอนิกส์ให้เกิดความสมดุลระหว่างค่าใช้จ่ายและผลประโยชน์ของสถาบันการเงิน ผู้ใช้บริการ และผู้ที่เกี่ยวข้องในการโอนเงินทางอิเล็กทรอนิกส์ โดยวิเคราะห์จากเอกสาร รายงาน บันทึก ตราสารอื่นๆ ซึ่งเป็นสิ่งจำเป็นที่มีผลกระทบต่อการแข่งขันระหว่างการให้บริการธนาคารอิเล็กทรอนิกส์ ทั้งสถาบันการเงินขนาดใหญ่และสถาบันการเงินขนาดเล็กซึ่งให้บริการแก่ผู้ใช้บริการในแต่ละประเภท
3. การกำหนดค่าใช้จ่ายระหว่างผู้ใช้บริการทางการเงิน และสถาบันทางการเงินโดยมุ่งคุ้มครองผู้ใช้บริการทางการเงินการธนาคาร

4. การกำหนดให้คณะกรรมการกลางมีอำนาจกำหนดกฎเกณฑ์ หรืออนุมาตราต่างๆ เพื่อกำหนดรูปแบบของการรายงานหรือการเปิดเผยข้อมูลของการโอนเงินทางอิเล็กทรอนิกส์ ให้เหมาะสมกับรูปแบบการให้บริการโอนเงินทางอิเล็กทรอนิกส์ในแต่ละประเภท
5. การกำหนดให้คณะกรรมการกลางมีอำนาจแก้ไข หรือกำหนดข้อยกเว้นสำหรับการโอนเงินทางอิเล็กทรอนิกส์บางประเภทได้ เพื่อให้สอดคล้องกับแนวทางปฏิบัติของธนาคารหรือสถาบันทางการเงิน ซึ่งกรณีดังกล่าวเป็นกรณีจำเป็นในการบรรเทาหรือลดการกระทำอันผิดต่อกฎหมาย หรือให้สอดคล้องกับการควบคุมการโอนเงินทางอิเล็กทรอนิกส์ให้เป็นไปด้วยความเรียบร้อย
6. การกำหนดหลักปฏิบัติให้แก่ผู้ให้บริการทางการเงินการธนาคารรายอื่น ๆ นอกเหนือจากธนาคารหรือสถาบันทางการเงินในการเปิดเผยข้อมูล การคุ้มครองการให้บริการทางการโอนเงินทางอิเล็กทรอนิกส์เพื่อให้การควบคุมการโอนเงินทางอิเล็กทรอนิกส์ของผู้ให้บริการแต่ละประเภทมีหลักปฏิบัติที่เป็นไปในแนวทางเดียวกัน
7. กฎ ระเบียบ อนุมาตราต่างๆ ที่กำหนดขึ้นโดยคณะกรรมการกลาง คณะกรรมการกลางจะต้องส่งให้รัฐสภาพิจารณาโดยเร็ว[4]
8. สถาบันทางการเงิน หรือธนาคารจะต้องจัดทำสรุปรายงานการเคลื่อนไหวทางบัญชีอิเล็กทรอนิกส์ หรือการเดินสะพัดแห่งบัญชีในการโอนเงินทางอิเล็กทรอนิกส์ อย่างน้อยปีละหนึ่งครั้ง[5]

3.1.1.1.2. การเปิดเผยข้อมูล

พระราชบัญญัติฉบับนี้กำหนดให้การโอนเงินทางอิเล็กทรอนิกส์ต้องมีการเปิดเผยข้อมูลด้วยภาษาที่เข้าใจได้ง่าย ไม่ว่าจะเป็นการกำหนดให้มีการเปิดเผยข้อมูล

---

[4] United State Code, (Title 15 : Commerce and Trade, Chapter 41 : Consumer Credit Protection, Subchapter VI : Electronic Fund Transfers, section 1693 (b) (4)). [online] Available from : http://caselaw.lp.findlaw.com.

[5] Ibid., section 1693c (a)(7).

โดยธนาคารหรือสถาบันทางการเงินหรือโดยผู้ใช้บริการ ซึ่งการเปิดเผยข้อมูลของการโอนเงินทางอิเล็กทรอนิกส์มีรายละเอียดดังนี้

1. ธนาคาร หรือสถาบันทางการเงินมีหน้าที่เปิดเผยข้อมูลในการโอนเงินทางอิเล็กทรอนิกส์แก่ผู้ใช้บริการ ในกรณีดังต่อไปนี้

1.1 ผู้ใช้บริการจะต้องได้รับรายงานเอกสารหรือใบบันทึกรายการที่ได้ทำการโอนเงินทางอิเล็กทรอนิกส์ ณ เวลาที่ทำการโอนเงินทางอิเล็กทรอนิกส์ โดยใบบันทึกรายการหรือรายงานเอกสารดังกล่าวต้องมีข้อมูลต่อไปนี้

1.1.1 จำนวนเงินหรือวันที่โอน

1.1.2 ประเภทของการโอน

1.1.3 บัญชีธนาคารของผู้ใช้บริการหรือผู้โอน และบัญชีผู้รับประโยชน์หรือผู้รับโอน

1.1.4 ข้อมูลเฉพาะของบุคคลที่สาม กรณีผู้รับโอนทำการโอนเงินให้บุคคลที่สาม

1.1.5 พื้นที่ที่ทำการโอน[6]

1.2 กรณีบัญชีที่มีสมุดบัญชี ธนาคารหรือสถาบันทางการเงินต้องจัดสมุดบัญชีที่สามารถทำรายการทางบัญชีผ่านสมุด เพื่อการแสดงรายละเอียดของจำนวนเงิน วันที่ หรือรายการเดินสะพัดทางบัญชีของการโอนเงินทางอิเล็กทรอนิกส์ ตั้งแต่การบันทึกรายการครั้งสุดท้ายจนถึงการบันทึกรายการปัจจุบัน[7]

1.3 กรณีบัญชีที่ไม่มีสมุดบัญชี และผู้ใช้บริการได้ทำการโอนเงินทางอิเล็กทรอนิกส์ ธนาคารหรือสถาบันทางการเงินต้องจัดทำใบบันทึกรายการเบื้องต้นให้แก่ผู้ใช้บริการ อย่างน้อยเดือนละครั้ง หรือในรอบระยะเวลาบัญชีที่มีการโอนเงินทางอิเล็กทรอนิกส์เกิดขึ้น ซึ่งอาจเป็นรอบระยะเวลาบัญชีที่มีความเคลื่อนไหวทางบัญชีทุก ๆ สามเดือนหรืออาจมากกว่านั้น โดยใบบันทึกรายการดังกล่าวต้องมีข้อมูลเกี่ยวกับการโอนเงินทาง

---

[6] United State Code, (Title 15 : Commerce and Trade , Chapter 41 : Consumer Credit Protection, Subchapter VI : Electronic Fund Transfers, section 1693 d (a)). [online] Available from : http://caselaw.lp.findlaw.com.

[7] Ibid., Section 1693 d (d).

อิเล็กทรอนิกส์ที่ชัดเจนประกอบ นอกเหนือข้อมูลในการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งมีรายละเอียดดังนี้

1.3.1 ข้อมูลที่เกี่ยวข้องกับข้อมูลในรายงานเอกสาร หรือใบบันทึกรายการ

1.3.2 จำนวนเงินของค่าธรรมเนียมหรือเงินที่สถาบันการเงินประเมินไว้สำหรับการทำรายการโอนเงินทางอิเล็กทรอนิกส์ หรือค่ารักษาบัญชี

1.3.3 รายการทางบัญชีของผู้ใช้บริการ ณ เวลาหนึ่งจนถึงอีก ณ เวลาหนึ่ง

1.3.4 ที่อยู่และหมายเลขโทรศัพท์ของสถาบันทางการเงินหรือธนาคาร เพื่อวัตถุประสงค์ติดต่อของผู้ใช้บริการไม่ว่ากรณีใด หรือหากมีข้อผิดพลาดทางบัญชีของผู้ใช้บริการเกิดขึ้น ซึ่งที่อยู่และหมายเลขโทรศัพท์นั้นต้องแจ้งว่า "ติดต่อโดยตรง:" หรือข้อความอย่างอื่นที่แสดงความหมายเช่นนั้น เพื่อให้เข้าใจได้ว่าที่อยู่และหมายเลขโทรศัพท์ดังกล่าวใช้ในติดต่อธนาคารหรือสถาบันทางการเงินนั้นโดยตรง[8]

1.4 บัญชีที่นอกเหนือจากบัญชีที่มีสมุดธนาคารและไม่อาจทำการโอนเงินทางอิเล็กทรอนิกส์ได้โดยปกติทั่วไป ธนาคารหรือสถาบันทางการเงินต้องจัดให้มีรายงานการเงินในแต่ละไตรมาส (หรือทุกสามเดือน) ที่แสดงถึงรายการทางบัญชีเช่นเดียวกับรายการทางบัญชีที่ต้องแสดงในใบบันทึกรายการเบื้องต้น[9]

1.5 กรณีการโอนเงินทางอิเล็กทรอนิกส์ล่วงหน้า ไม่ว่าจะเป็นการโอนเงินผ่านบัตรเครดิต หรือการโอนผ่านบัตรเดบิตของบัญชีสินเชื่อหรือบัญชีที่ให้วงเงินเบิกเกินบัญชี ธนาคารหรือสถาบันทางการเงินต้องจัดทำใบบันทึกรายการดังกล่าว

---

[8] United State Code, (Title 15 : Commerce and Trade ; Chapter 41 : Consumer Credit Protection, Subchapter VI : Electronic Fund Transfers , section 1693 d (c). [online] Available from : http://caselaw.lp.findlaw.com.

[9] Ibid., section 1693 d (e).

และจัดส่งให้แก่ผู้ใช้บริการอย่างน้อยหนึ่งครั้งภายในรอบระยะเวลา 60 วัน [10]

2. ผู้ใช้บริการโอนเงินทางอิเล็กทรอนิกส์ต้องเปิดเผยข้อมูลที่ถูกต้องของตนแก่ธนาคารหรือสถาบันทางการเงิน กล่าวคือ ผู้ใช้บริการการโอนเงินทางอิเล็กทรอนิกส์ต้องแจ้งหมายเลขโทรศัพท์ หรือที่อยู่ที่ถูกต้องของตนแก่ธนาคาร หรือสถาบันทางการเงิน ณ เวลาที่ทำการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าว
3. ธนาคารหรือสถาบันทางการเงินสามารถแจ้งหมายเลขโทรศัพท์หรือที่อยู่ของบุคคลหรือสำนักงานที่ผู้ใช้บริการเชื่อว่าเป็นผู้ดำเนินการโอนเงินอิเล็กทรอนิกส์โดยปราศจากอำนาจได้ ไม่ว่าจะเป็นประเภทหรือลักษณะของการโอนเงินทางอิเล็กทรอนิกส์ จำนวนครั้งหรือจำนวนเงินที่โอนดังกล่าว ยกเว้นรายละเอียดที่ไม่ต้องถูกเปิดเผยหรือเป็นความลับที่เกี่ยวกับความปลอดภัยของระบบการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งจะถูกกำหนดไว้โดยคณะกรรมการกลาง[11]
4. สถาบันทางการเงินหรือธนาคารอาจมีการเปิดเผยข้อมูลของผู้ใช้บริการในการโอนเงินทางอิเล็กทรอนิกส์ได้ในกรณีที่เพื่อประโยชน์ในทางธุรกิจแก่บุคคลที่สาม
5. กรณีที่มีความเปลี่ยนแปลงรูปแบบ หรือเงื่อนไขทางบัญชีของผู้ใช้บริการที่ต้องเปิดเผยข้อมูล ตามที่ได้กำหนดไว้ในพระราชบัญญัติฉบับนี้ และความเปลี่ยนแปลงดังกล่าวอาจมีผลกระทบและทำให้เกิดรับผิดแก่ผู้บริโภคมากขึ้น สถาบันทางการเงินต้องแจ้งรูปแบบเงื่อนไขทางบัญชีแก่ผู้ใช้บริการโดยปราศจากเงื่อนไขโดยทันที หรืออย่างน้อย 21 วัน ทั้งนี้กรณีดังกล่าวต้องเป็นไปเพื่อความปลอดภัยของระบบการโอนเงินทางอิเล็กทรอนิกส์[12]
6. หากสถาบันทางการเงินทำการแจ้งหรือบอกกล่าวอย่างครบถ้วนโดยทันทีหรือโดยพลัน ในกรณีที่มีความผิดพลาด, การลักขโมย หรือการ

---

[10] United State Code, (Title 15 : Commerce and Trade, Chapter 41 : Consumer Credit Protection, Subchapter VI : Electronic Fund Transfers, section 1693 d (b)). [online] Available from : http://caselaw.lp.findlaw.com.

[11] Ibid., section 1693c (a)(2).

[12] Ibid., section 1693c (b).

ใช้บัตรที่มีแถบแม่เหล็กหรือรหัสโดยปราศจากอำนาจ หรือการเข้าถึงโดยวิธีหนึ่งวิธีใด (กรณีนี้ผู้ใช้บริการจึงจะไม่ต้องรับผิดในกรณีดังกล่าว)[13]

<u>บทกำหนดโทษ</u>

ผู้ใดกระทำการฝ่าฝืนมาตรการในการป้องกัน และปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ข้างต้น กล่าวคือ

- การแจ้งข้อความอันเป็นเท็จ หรือการแจ้งข้อความไม่ตรงกับความจริงในการรายงานการโอนเงินทางอิเล็กทรอนิกส์
- การฝ่าฝืน ละเลย หรือเพิกเฉยการแจ้งหรือรายงานการโอนเงินทางอิเล็กทรอนิกส์
- การฝ่าฝืน ละเลย หรือเพิกเฉยการปฏิบัติตามมาตรการทางกฎหมายต่างๆ ที่ได้กำหนดไว้ดังที่ได้อธิบายแล้วข้างต้น

ผู้นั้น มีโทษปรับ ไม่เกิน 5,000 ดอลลาร์สหรัฐ หรือ โทษจำคุกไม่เกินหนึ่ง ปี หรือทั้งจำทั้งปรับ

3.1.1.2 พระราชบัญญัติความลับทางธนาคาร (Bank Secrecy Act)

พระราชบัญญัติความลับทางธนาคารเป็นบทบัญญัติที่วางมาตรการทางกฎหมายแก่ธนาคาร หรือสถาบันทางการเงินในการจัดทำบันทึกหรือรายงานในการทำธุรกรรมทางการเงินการธนาคารลักษณะต่างๆ และรวมถึงการโอนเงินทางอิเล็กทรอนิกส์โดยทั่วไป เพื่อให้ทราบแหล่งที่มาของเงิน ปริมาณเงิน และความเคลื่อนไหวของกระแสการเงินที่นำเข้าหรือนำออกนอกประเทศ หรือที่ฝากไว้ในธนาคารหรือสถาบันการเงิน เพื่อช่วยให้เจ้าหน้าที่ของรัฐสามารถตรวจสอบและสืบสวนผู้กระทำความผิดดังล่าวได้ ด้วยสาเหตุว่าการโอนเงินทางอิเล็กทรอนิกส์ถือเป็นข้อมูลของธนาคารเป็นความลับ ธนาคารไม่สามารถเปิดเผยข้อมูลในบัญชีของลูกค้าได้ การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตจึงถือเป็นความผิดทางอาญา ซึ่ง

---

[13] <u>United State Code</u>,(Title 15 : Commerce and Trade, Chapter 41 : Consumer Credit Protection, Subchapter VI : Electronic Fund Transfers, section 1693c (a)(1)). [online] Available from : <u>http://caselaw.lp.findlaw.com</u>.

บางกรณีเจ้าหน้าที่ของสถาบันทางการเงินหรือธนาคารมักไม่ได้รับความร่วมมือจากธนาคารในต่างประเทศในการติดตามพฤติการณ์ของผู้ฝากเงินเพื่อการฟอกเงิน หรือการกระทำความผิดในลักษณะอื่นๆ ที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ดังนั้นมาตรการในการป้องกันและปราบปรามอาชญากรรมดังกล่าวจึงล้วนแล้วแต่ต้องอาศัยข้อมูลทางธนาคารเป็นปัจจัยสำคัญในการติดตามการกระทำความผิดลักษณะดังกล่าว

ตามพระราชบัญญัติความลับทางธนาคาร ซึ่งได้บัญญัติไว้ในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 31 การเงินและการธนาคาร ลักษณะ 53 ธุรกรรมทางการเงิน หมวดที่ 2 บันทึกและรายงานในการทำธุรกรรมทางการเงิน และหมวดที่ 3 การฟอกเงินและอาชญากรรมที่เกี่ยวข้องกับการธนาคาร ตั้งแต่มาตรา 5311-5315 (Title 31 - Money and Finance, Chapter 53 - Monetary Transaction, in particular, Subchapter II – Records and Reports on money Instruments Transaction and Subchapter III – Money Laundering and Related Financial Crimes, Section 5311-5355) บทบัญญัติดังกล่าวได้กำหนดมาตรการทางกฎหมายที่เป็นกฎเกณฑ์เกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งจัดเป็นมาตรการในการป้องกันและปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ได้ โดยมีสาระสำคัญ [14] ดังนี้

3.1.1.2.1 การรายงานธุรกรรมทางการเงิน

การโอนเงินทางอิเล็กทรอนิกส์ ได้มีการกำหนดให้ต้องมีการรายงานการโอนเงินดังกล่าว ซึ่งอาจสรุปเป็นแต่ละกรณีได้ดังนี้

1. บุคคลหรือนิติบุคคลที่ทำการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งมีจำนวนเกินกว่า 10,000 ดอลลาร์สหรัฐขึ้นไป ต้องรายงานธุรกรรมหรือความสัมพันธ์ที่มีต่อสถาบันทางการเงินหรือธนาคาร ตามหลักเกณฑ์ที่รัฐมนตรีว่าการกระทรวงการคลังกำหนด และบุคคลหรือตัวแทนหรือผู้รับฝากเงินต้องรายงานการนำเงินหรือตราสารทางการเงิน

---

[14] Bank Secrecy Act ,(Title 31 : Money and Finance, Chapter 53 : Monetary Transaction, Subchapter II – Records and Reports on money Instruments Transaction, section 5311-5315). [online] Available from : http://www4.law.cornell.edu/uscode/html.

2. สถาบันทางการเงิน หรือตัวแทน หรือผู้รับฝากเงินต้องรายงานการโอนเงิน ไม่ว่ากรณีการโอนเงินหรือตราสารทางการเงินซึ่งมีจำนวนเกินกว่า 10,000 ดอลลาร์สหรัฐ หรือมากกว่านั้น
3. สถาบันทางการเงินต้องรายงานการจ่ายเงิน การรับเงิน หรือการโอนเงินตามที่รัฐมนตรีว่าการกระทรวงการคลังกำหนด ซึ่งมีจำนวนเกินกว่า 10,000 ดอลลาร์สหรัฐ หรือมากกว่านั้น

3.1.1.2.3 การจัดเก็บบันทึก หรือไฟล์รายงานการโอนเงินทางอิเล็กทรอนิกส์

รัฐมนตรีว่าการกระทรวงการคลังได้กำหนดให้ธนาคารหรือสถาบันทางการเงินต้องจัดเก็บบันทึก หรือไฟล์รายงานการโอนเงินทางอิเล็กทรอนิกส์ โดยบันทึกหรือรายงานดังกล่าวอาจเก็บเป็นบันทึกเอกสารหรือไฟล์รายงาน ซึ่งข้อมูลตามบันทึกหรือรายงานการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าวต้องประกอบด้วยข้อมูลต่อไปนี้

1. ชื่อ คุณสมบัติเฉพาะ และที่อยู่ของผู้ที่เกี่ยวข้องในกระบวนการโอนเงินทางอิเล็กทรอนิกส์
2. ประเภทบัญชีที่ทำการโอนเงินทางอิเล็กทรอนิกส์

3.1.1.2.4 การให้ข้อมูลทางการเงินกับหน่วยงานอื่นๆ ของรัฐตามความจำเป็นและความเหมาะสม

กำหนดให้อำนาจรัฐมนตรีว่าการกระทรวงการคลังในการสั่งให้สถาบันทางการเงินอาจทำการกระจายข้อมูลหรือรายการทางบัญชี เพื่อประโยชน์แก่หน่วยงานอื่นๆ ในการสืบสวนสอบสวน หรือดำเนินคดีอาญา หรือคดีภาษีอากร และข้อมูลที่ได้รับนั้นต้องถูกเก็บรักษาไว้เป็นความลับ และเป็นการเปิดเผยเพื่อใช้ในทางราชการเกี่ยวกับการสืบสวนสอบสอบและดำเนินคดี

3.1.1.2.5 การโอนเงินทางอิเล็กทรอนิกส์ต้องอยู่ภายใต้ของหลักการให้ลูกค้าแสดงตนเสมอ

ธนาคารหรือสถาบันทางการเงินต้องอบรมให้เจ้าหน้าที่ พนักงานธนาคาร หรือลูกจ้างธนาคารสามารถเข้าใจได้ถึงเหตุผลและหลักการปฏิบัติเกี่ยวกับการให้ลูกค้าแสดงตน หรือการบันทึกรายงานข้อมูลทางการเงิน การให้ความร่วมมือในการตรวจสอบข้อมูลในลักษณะต่างๆ โดยหลักการดังกล่าวอยู่บนพื้นฐานของบทบัญญัติในการบังคับใช้กับข้อมูลในบันทึกหรือรายงานการโอนเงินทางอิเล็กทรอนิกส์ที่กล่าวข้างต้นจะเห็นได้ว่า เป็นไปตามหลักปฏิบัติที่เหมาะสมของธนาคารว่า "หลักการให้ลูกค้าแสดงตน (know your customer)" กล่าวคือ

1. การตรวจสอบความถูกต้องของข้อมูลเฉพาะ ของลูกค้าตั้งแต่มาทำการเปิดบัญชี
2. การเก็บบันทึกหรือรายงานในการโอนเงินไว้
3. การตรวจสอบชื่อของลูกค้ากับรัฐบาล หรือหน่วยงานสืบสวนสอบสวนของรัฐว่าจัดอยู่ในรายชื่อของผู้ก่อการร้าย อาชญากร หรือบุคคลที่น่าต้องสงสัยหรือไม่
4. ข้อมูลที่ต้องขอจากลูกค้าได้แก่ ชื่อ นามสกุล ที่อยู่ อาชีพ หนังสือเดินทาง บัตรประกันสังคม หรือใบขับขี่รถยนต์ หมายเลขประจำตัวผู้เสียภาษี และข้อมูลอื่นๆ ที่เกี่ยวข้องกับที่มาของเงินดังกล่าว

<u>บทกำหนดโทษ</u>

1. หากสถาบันทางการเงินหรือผู้มีอำนาจหน้าที่จงใจฝ่าฝืนกฎหมายหรือระเบียบที่ออกภายใต้กฎหมายนี้ จะต้องถูกปรับมากกว่าจำนวนเงินที่เกี่ยวข้องกับธุรกรรม หรือปรับ 25,000 ดอลลาร์สหรัฐ หรือไม่เกิน 100,000 ดอลลาร์สหรัฐ
2. หากผู้ใดเจตนาฝ่าฝืนกฎหมาย หรือระเบียบที่ออกภายใต้กฎหมายดังกล่าวจะถูกปรับไม่เกิน 250,000 ดอลลาร์สหรัฐ หรือ โทษจำคุกไม่เกิน ห้า ปี หรือทั้งจำทั้งปรับ
3. หากผู้ใดเจตนาฝ่าฝืนกฎหมาย หรือระเบียบปฏิบัติข้างต้น โดยการโอนเงินดังกล่าวมีมูลค่าเกินกว่า 100,000 ดอลลาร์สหรัฐ ใน

ระยะเวลา 12 เดือน ผู้ฝ่าฝืนกรณีดังกล่าวต้องมีโทษปรับไม่เกิน 500,000 ดอลลาร์สหรัฐ หรือจำคุกไม่เกิน 10 ปีหรือทั้งจำทั้งปรับ

3.1.1.3 พระราชบัญญัติต่อต้านการฟอกเงินระหว่างประเทศและต่อต้านการก่อการร้าย ค.ศ. 2001 (International Money Laundering Abatement Act : IMLA)

พระราชบัญญัติต่อต้านการฟอกเงินระหว่างประเทศและต่อต้านการก่อการร้าย ค.ศ. 2001 เป็นบทบัญญัติหนึ่งของพระราชบัญญัติการต่อต้านการก่อการร้ายแห่งประเทศสหรัฐอเมริกา ลักษณะที่ 3 ว่าด้วยการต่อต้านการฟอกเงินระหว่างประเทศและต่อต้านการก่อการร้าย (H.R.3162 USA Patriot Act, 2001,Title III – The International Money Laundering Abatement and Anti-Terrorist Financial) ซึ่งได้บัญญัติขึ้นเมื่อวันที่ 26 ตุลาคม 2541 โดยเป็นผลอันเนื่องมาจากการก่อวินาศกรรม เมื่อวันที่ 11 กันยายน 2541 ที่มีการก่อการร้ายโจมตีนิวยอร์ค วอชิงตัน.ดีซี และเพนซิวาเนีย ซึ่งเหตุการณ์ดังกล่าวทำให้ประเทศสหรัฐอเมริกาให้ความสำคัญกับมาตรการทางกฎหมายในการต่อต้านการก่อการร้าย และการต่อต้านการฟอกเงินมากขึ้น[15]

พระราชบัญญัติฉบับนี้เป็นบทบัญญัติในการวางมาตรการต่างๆ ในการบังคับใช้กับการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ให้ถือว่าเป็นการก่อการร้ายต่อระบบการเงินการธนาคาร ดังนั้นจึงเป็นความจำเป็นในการแก้ไขเพิ่มเติมพระราชบัญญัติความลับทางธนาคาร (The Bank Secrecy Act : BSA) ให้สามารถบังคับใช้กับกรณีของการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ภายใต้กฎหมายแห่งประเทศสหรัฐอเมริกาได้อย่างมีประสิทธิภาพมากขึ้น

โดยหากพิจารณาเฉพาะมาตรการทางกฎหมายในการป้องกันและปราบปรามการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ตามพระราชบัญญัติฉบับนี้มีสาระสำคัญ ดังนี้

---

[15] Kevin F. Barnard and Kathlee A. Scott. Correspondent Banking A Major Focus Of The New USA Patriot Act. (White & Case Limited Liability Partnership). [online] Available from : http://www.whitecase.com/bank_compliance.html.

3.1.1.3.1 กำหนดมาตรการพิเศษในการบันทึกหรือรายงานการโอนเงินทางอิเล็กทรอนิกส์ซึ่งอาจเกี่ยวเนื่องกับการฟอกเงินโดยการโอนเงินทางอิเล็กทรอนิกส์

ซึ่งบทบัญญัตินี้ได้กำหนดเพิ่มเติมให้รัฐมนตรีว่าการกระทรวงการคลังมีอำนาจในการเรียกบันทึกหรือรายงานการโอนเงินทางอิเล็กทรอนิกส์จากสถาบันทางการเงินหรือตัวแทนหรือผู้ที่ได้รับอนุญาตได้ ตามมาตรา 5318 A แห่งพระราชบัญญัติความลับทางการเงิน กรณีหากสงสัยว่ามีพฤติการณ์เบื้องต้นแห่งการฟอกเงินโดยการโอนเงินทางอิเล็กทรอนิกส์[16]

3.1.1.3.2 การเชื่อมโยงข้อมูลระหว่างธนาคารได้อย่างทั่วถึง

ธนาคาร หรือสถาบันทางการเงินที่ให้บริการทางด้านการเงินการธนาคารต้องจัดให้มีการเชื่อมโยงข้อมูลทางบัญชีผ่านหน้าจอระหว่างธนาคาร หรือสถาบันทางการเงินได้อย่างใกล้ชิดและรวดเร็วที่สุด ไม่ว่าจะเป็นการโอนเงินทางอิเล็กทรอนิกส์ภายนอกประเทศหรือการโอนเงินภายในประเทศสหรัฐอเมริกา[17]

3.1.1.3.3 มาตรการพิเศษในการเรียกข้อมูลการโอนเงินทางอิเล็กทรอนิกส์จากธนาคารต่างประเทศ

ตามบทบัญญัติฉบับนี้ และกรณีเป็นที่สงสัยว่าการกระทำดังกล่าวเป็นการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ภายใต้การโอนเงินระหว่างธนาคารต่างประเทศ และพระราชบัญญัตินี้ได้กำหนดให้ รัฐมนตรีว่าการกระทรวงการคลังสามารถขอเรียกข้อมูลการโอนเงิน ซึ่งถือเป็นข้อมูลความลับทางธนาคารจากธนาคารต่างประเทศได้

---

[16] USA PATRIOT ACT, section 311, adding section 5318A of Bank Secrecy Act. [online] Available from : http://www.whitecase.com/bank_compliance.html.

[17] Ibid., Section 302., adding section 5318A of Bank Secrecy Act.

3.1.1.2.4 การจัดโปรแกรมการต่อต้านการฟอกเงินเบื้องต้น (Anti-Money Laundering Programs: 31 U.S.C. 5318 (h), adding by USA Patriot Act)

พระราชบัญญัติฉบับนี้ กำหนดให้ธนาคารหรือสถาบันทางการเงินจัดสร้างโปรแกรมการต่อต้านการฟอกเงินเบื้องต้น ภายใต้การโอนเงินทางอิเล็กทรอนิกส์ของระบบการเงินการธนาคาร นอกเหนือจากการธนาคารหรือสถาบันทางการเงินต้องจัดทำบันทึกหรือจัดเก็บรายงานในการโอนเงินทางอิเล็กทรอนิกส์แล้ว ซึ่งโปรแกรมการต่อต้านการฟอกเงินดังกล่าวกำหนดให้ธนาคารหรือสถาบันทางการเงินต้องปฏิบัติดังต่อไปนี้

1. การพัฒนาวิธีการดำเนินการ การควบคุม และนโยบายการจัดการการฟอกเงินภายในประเทศ
2. การแต่งตั้งพนักงานที่มีหน้าที่ในการให้ความร่วมมือกับเจ้าพนักงานของรัฐที่มีอำนาจหน้าที่ในการป้องกันการฟอกเงินดังกล่าว
3. การจัดโปรแกรมการฝึกอบรมพนักงานหรือลูกจ้างธนาคารในเรื่องดังกล่าว
4. การจัดทำโปรแกรมที่ทำหน้าที่ตรวจสอบโดยอิสระ[18]

<u>บทกำหนดโทษ</u>

1. หากสถาบันทางการเงินหรือผู้มีอำนาจหน้าที่จงใจฝ่าฝืนกฎหมาย หรือระเบียบที่ออกภายใต้กฎหมายนี้ผู้นั้นจะต้องถูกปรับมากกว่าจำนวนเงินที่เกี่ยวข้องกับธุรกรรมนั้น หรือปรับ 25,000 ดอลลาร์สหรัฐ หรือไม่เกิน 100,000 ดอลลาร์สหรัฐ
2. หากผู้ใดเจตนาฝ่าฝืนกฎหมาย หรือระเบียบที่ออกภายใต้กฎหมายดังกล่าวจะถูกปรับไม่เกิน 250,000 ดอลลาร์สหรัฐ หรือ โทษจำคุก ไม่เกิน ห้า ปี หรือทั้งจำทั้งปรับ

---

[18] <u>USA PATRIOT ACT</u>, section 352, adding section 5318A of Bank Secrecy Act. [online] Available from : <u>http://www.whitecase.com/bank_compliance.html</u>.

3. หากผู้ใดเจตนาฝ่าฝืนกฎหมาย หรือระเบียบปฏิบัติข้างต้น โดยการโอนเงินดังกล่าวมีมูลค่าเกินกว่า 100,000 ดอลลาร์สหรัฐภายในระยะเวลา 12 เดือน ผู้ฝ่าฝืนกรณีดังกล่าวต้องมีโทษปรับไม่เกิน 500,000 ดอลลาร์สหรัฐ หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ

3.1.2 ประเทศสหราชอาณาจักร (United Kingdom)

ประเทศสหราชอาณาจักรถือว่าเป็นศูนย์กลางทางการเงินการธนาคารที่สำคัญที่สุดแห่งหนึ่ง และเป็นประเทศผู้นำของกลุ่มสหภาพยุโรป (European Union) ในการกำหนดมาตรการทางกฎหมายป้องกันและปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ไว้ในพระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceeds of Crimes Act, 2002) โดยเฉพาะการต่อต้านการฟอกเงินโดยการโอนเงินทางการเงินการธนาคารหรือการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งแม้ว่าความผิดเกี่ยวกับยาเสพติดจะเป็นความผิดหลักในการฟอกเงินแต่ปัจจุบันได้มีความผิดเกี่ยวกับการฉ้อโกงทางสถาบันทางการเงินหรือการลักลอบขนส่งสินค้าได้กลายเป็นความผิดสำคัญและมีแนวโน้มเพิ่มมากขึ้นอย่างรวดเร็ว โดยเฉพาะแนวโน้มของการโอนเงินผ่าน ธนาคารและ สถาบันทางการเงินหลักของประเทศ และความผิดต่อการฟอกเงินโดยการโอนเงินที่เกิดขึ้นในปัจจุบันจะกระทำโดยจะอาศัยการแลกเปลี่ยนเงินตราต่างประเทศ หรือการลักลอบโอนเงินออกนอกประเทศ เพื่อปกปิดที่มาของเงินที่ได้มาจากการกระทำความผิด

ประกอบกับ การให้บริการทางการเงินการธนาคารของประเทศสหราชอาณาจักรจัดแบ่งลักษณะทางบัญชีออกได้ 2 ลักษณะ กล่าวคือ บัญชีที่มีลักษณะทางบัญชี (residents) และบัญชีที่ไม่มีลักษณะทางบัญชี (nonresidents) โดยประเทศสหราชอาณาจักรได้ขยายการให้บริการทางธนาคารให้สามารถเปิดบัญชีธนาคารได้หลากหลายวิธีการ รวมไปถึงบัญชีที่ไม่มีลักษณะทางบัญชีซึ่งจะเป็นบัญชีที่เปิดทางด้านอินเทอร์เน็ตหรือการให้บริการบัญชีในรูปแบบอื่นๆ ด้วยเหตุนี้จึงเป็นสาเหตุให้บัญชีธนาคารประเภทที่ไม่มีลักษณะทางบัญชีจึงมีความซับซ้อนในการตรวจสอบข้อมูลสำคัญทางบัญชี หรือการตรวจสอบการกระทำอันเป็นความผิด

หากพิจารณาถึงมาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ของประเทศสหราชอาณาจักรนั้น มีสาระสำคัญดังนี้

3.1.2.1 พระราชบัญญัติธนาคารกลางแห่งสหราชอาณาจักร ค.ศ. 1988 (The Bank of England Act, 1998)

พระราชบัญญัติธนาคารกลางแห่งสหราชอาณาจักร ค.ศ. 1998 (The Bank of England Act, 1998) ซึ่งเป็นบทบัญญัติแก้ไขเพิ่มเติมพระราชบัญญัติธนาคารกลางแห่งสหราชอาณาจักร ค.ศ. 1987 โดยได้วางข้อกำหนดในการจัดตั้ง วางกฎเกณฑ์ หรือการจัดการทางด้านการธนาคาร และกำหนดหน้าที่ของธนาคารแห่งสหราชอาณาจักร รวมไปถึงอำนาจหน้าที่ของผู้ที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ และกฎหมายฉบับดังกล่าวได้วางข้อกำหนดให้มีการจัดทำรายการและเก็บรักษาข้อมูลทางการโอนเงินนั้นไว้ซึ่งเป็นไปตามข้อกำหนดของบาเซิล (Basel Committee) ที่เป็นมาตรฐานของธนาคารกลางระหว่างประเทศ (Bank for International Settlement)[19] กล่าวคือ

1.1 การให้ลูกค้าแสดงตนที่แท้จริงในการให้ข้อมูลที่ถูกต้องของตนในการโอนเงินทางอิเล็กทรอนิกส์

1.2 การปฏิบัติตามกฎ ระเบียบข้อบังคับที่ใช้บังคับเรื่องการจัดเก็บข้อมูลทางการโอนเงิน และรายงานการโอนเงิน ตามมาตรา17 [20]กล่าวคือ

1.2.1 ธนาคารหรือสถาบันทางการเงินต้องเก็บข้อมูลเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์เท่าที่จำเป็นต่อการปฏิบัติหน้าที่ของธนาคารหรือสถาบันทางการเงิน

1.2.2 การจัดทำบันทึกการโอนเงินดังกล่าวต้องจัดทำเป็นลายลักษณ์อักษร และประกอบด้วยข้อมูลเฉพาะของประเภทการโอน ระยะเวลา สถานที่ ตลอดจนข้อมูลทางบัญชี และข้อมูลเฉพาะของลูกค้า

1.3 การให้ความร่วมมือกับพนักงานเจ้าหน้าที่ผู้รักษากฎหมาย โดยให้ข้อมูลของลูกค้าเท่าที่จะทำให้ได้ ซึ่งได้กำหนดขอบเขตในการเปิดเผย

---

[19] U.S. Department of State. Money Laundering and Financial Crimes. in part of United Kingdom (Primary). [online] Available from : http://www.state.gov/g/inl/ris/nrcrpt/2000/959.html.

[20] Bank of England Act, 1998 , section 17. [online] Available from : http://www.bankofengland.co.uk./legislation/main.html.

ข้อมูลการโอนเงินทางอิเล็กทรอนิกส์กับพนักงานเจ้าหน้าที่ผู้รักษากฎหมายซึ่งเป็นไปตามมาตรา 37 ประกอบภาคผนวก 7 [21] กล่าวคือ

1.3.1 เพื่อประโยชน์ในทางธุรกิจ

1.3.2 เพื่อวัตถุประสงค์ในการปฏิบัติหน้าที่ของธนาคารหรือสถาบันทางการเงิน

1.3.3 เพื่อประโยชน์ในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่อื่นๆ

บทกำหนดโทษ

1.ความผิดอันเป็นการฝ่าฝืนการจัดเก็บหรือการทำรายงานของธนาคารที่กำหนดให้ต้องปฏิบัติตามมาตรา 17 (ตามมาตรา 38)[22] กล่าวคือ

1.1 หากธนาคารหรือสถาบันทางการเงินใดฝ่าฝืนไม่จัดถือข้อมูลทางการโอนเงิน หรือจัดทำรายงานการโอนเงินต่างๆ ผู้นั้นมีความผิดต้องโทษปรับไม่เกิน 2,000 ปอนด์ (ตารางระดับ 4)

1.2 หากผู้ใดถูกตัดสินให้มีความผิดข้างต้น และยังคงกระทำความผิดโดยให้การจัดเก็บข้อมูลและการจัดทำรายงานดังกล่าวล้มเหลว การกระทำดังกล่าวถือว่าผู้นั้นมีความผิด และผู้นั้นต้องมีโทษปรับตามสมควร

1.3 หากผู้ใดสมรู้ร่วมคิดหรือเจตนาให้ข้อมูลในทางบัญชีหรือการจัดทำรายงานดังกล่าวโดยรู้ว่าเป็นข้อมูลเท็จหรือไม่ตรงกับความจริง ผู้นั้นมีความผิดและต้องรับผิดโทษปรับตามสมควร หรือจำคุกไม่เกิน 2 ปี หรือทั้งจำทั้งปรับ หรือการพิจารณาคดีโดยรวบรัด ผู้นั้นต้องโทษจำคุกไม่เกิน 3 เดือน หรือปรับไม่เกินอัตราสูงสุด หรือทั้งจำทั้งปรับ

2. ผู้ใดฝ่าฝืนกฎ ระเบียบการเปิดเผยข้อมูลต่อพนักงานเจ้าหน้าที่ที่กำหนดไว้ ผู้นั้นมีความผิดนั้นมีความผิดและต้องรับผิดโทษปรับตามสมควร หรือจำคุกไม่เกิน 2 ปี หรือทั้งจำทั้งปรับ หรือการ

---

[21] Bank of England Act, 1998 , section 37 consist of Schedule 7. [online] Available from : http://www.bankofengland.co.uk./legislation/ main.html.

[22] Bank of England Act, 1998 , section 38. [online] Available from : http://www.bankofengland.co.uk./legislation/main.html

พิจารณาคดีโดยรวบรัด ผู้นั้นต้องโทษจำคุกไม่เกิน 3 เดือน หรือปรับไม่เกินอัตราสูงสุด หรือทั้งจำทั้งปรับ

3.1.2.2 พระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceeds of Crime Act, 2002)

พระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceeds of Crime Act) ซึ่งเป็นบทบัญญัติที่ได้มีการวาง กฎ ระเบียบต่างๆ ที่กำหนดให้สถาบันทางการเงินต้องวางมาตรการในการป้องกันและปรามปราบการกระทำอันเป็นการฟอกเงินทางการโอนเงินทางธนาคารอย่างเป็นระบบ ซึ่งถือเป็นมาตรการในการต่อต้านการฟอกเงิน (Anti-Money Laundering Strategy, 2000) โดยมาตรการดังกล่าวมีหลักการสอดคล้องกับมาตรการต่อต้านการฟอกเงินของสหภาพยุโรป และข้อเสนอแนะ 40 ประการของโครงการความร่วมมือระหว่างประเทศในการควบคุมอาชญากรรมทางการเงินการธนาคาร (Financial Action Task Forces) [23] ซึ่งพระราชบัญญัติฉบับดังกล่าวได้กำหนดสาระสำคัญเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ ไว้กล่าวคือ[24]

1. ธนาคารหรือสถาบันทางการเงินอื่นๆ จะต้องได้รับข้อมูลเฉพาะทางบัญชีของลูกค้าที่เกี่ยวข้องหรือลูกค้าที่ถือบัญชีดังกล่าว โดยข้อมูลเหล่านั้นเป็นข้อมูลที่ถือเป็นประโยชน์ในการสืบสวนสอบสวนคดี
2. ธนาคารหรือสถาบันทางการเงินอื่นๆ จะต้องจัดให้มีข้อมูลในการโอนเงินทางบัญชีที่เพียงพอแก่การควบคุม ขัดการการโอนเงิน หรือการดำเนินธุรกรรม ณ ช่วงเวลานั้น
3. ผู้โอนเงินทางอิเล็กทรอนิกส์มีหน้าที่ต้องเปิดเผยข้อมูลที่แท้จริงทั้งหมดที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าว หรือข้อมูลที่ธนาคารหรือสถาบันทางการเงินร้องขอในการดำเนินการโอนเงิน

---

[23] U.S. Department of State. Money Laundering and Financial Crimes. in part of United Kingdom (Primary). [online] Available from : http://www.state.gov/g/inl/ris/nrcrpt/2000/959.html.

[24] The Proceeds of Crime Act. [online] Available from : http://www.legal500.com/devs/uk/ cc/ukcc_002.html.

บทกำหนดโทษ

ผู้ใดละเลย หรือไม่ปฏิบัติตามการรายงานข้อมูลในการโอนเงินทางอิเล็กทรอนิกส์ข้างต้น หรือการทำให้เกิดความล้มเหลวในรายงานการโอนเงินทางอิเล็กทรอนิกส์ ไม่ว่าผู้นั้นจะเป็นธนาคารหรือสถาบันทางการเงิน พนักงานหรือเจ้าหน้าที่ของธนาคารหรือสถาบันทางการเงิน หรือผู้ที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าวฝ่ายใดฝ่ายหนึ่ง โดยให้ถือว่าผู้นั้นมีความผิด และผู้นั้นมีโทษปรับ หรือโทษจำคุกอัตราสูงสุด 5 ปี หรือทั้งจำทั้งปรับ

3.1.3 สหภาพยุโรป (European Union)

สหภาพยุโรปเป็นองค์กรความร่วมมือระหว่างประเทศของประเทศต่างๆ ในแถบทวีปยุโรป โดยมีสภาสหภาพยุโรป (Council of European) เป็นหน่วยงานสำคัญในการร่วมกันพิจารณา และออกอนุสัญญา สนธิสัญญา ข้อตกลง กฎ หรือคำสั่งต่างๆ เพื่อใช้บังคับภายในประเทศสมาชิกแห่งสหภาพยุโรป เพื่อเป็นการวางมาตรการในการควบคุม และกำกับดูแลในด้านต่างๆ ไม่ว่าจะเป็นด้านเศรษฐกิจ สังคม วัฒนธรรม วิทยาศาสตร์ กฎหมาย หรือการจัดการในด้านต่างๆ รวมถึงการคุ้มครองเสรีภาพและสิทธิมนุษยชนแห่งประเทศสมาชิกในสหภาพยุโรป ซึ่งคณะทำงานดังกล่าวจะมีการจัดตั้งคณะทำงานเฉพาะด้านต่างๆ เพื่อการกำกับ ดูแล และวางแนวทางปฏิบัติร่วมกันในกลุ่มประเทศสมาชิกของสหภาพยุโรปโดยเฉพาะ ซึ่งตามกฎบัตรของสภาสหภาพยุโรป (The Statue of the Council of Europe) มาตรา 1 ได้กำหนดให้ "สภาสหภาพยุโรปมีวัตถุประสงค์หลักในการดำเนินการประชุมร่วมกันในการกำหนดข้อตกลงหรือมาตรการต่างๆ ที่เกี่ยวกับเศรษฐกิจ สังคม วัตนธรรม วิทยาศาสตร์ กฎหมาย และการจัดการด้านต่างๆ และปกป้องคุ้มครองเสรีภาพและสิทธิมนุษยชน" [25]

โดยสภาสหภาพยุโรปได้มีการจัดตั้งธนาคารกลางยุโรป (European Central Bank) ขึ้น โดยอาศัยอำนาจแห่งสนธิสัญญาว่าด้วยการจัดตั้งองค์กรสหภาพยุโรป (Treaties on European Community) เพื่อเป็นหน่วยงานเฉพาะในการทำหน้าที่ควบคุม กำกับดูแลระบบการเงินการธนาคาร การค้าและการพาณิชย์แก่ประเทศสมาชิกแห่งสหภาพยุโรป และการกำกับดูแลด้านการเงินการธนาคาร ดังนั้นหน่วยงานดังกล่าวจึงได้มีประชุมร่วมกันในการยกร่างคำสั่งหรืออนุสัญญา เพื่อนำมาเป็นแนวทางทางด้านกฎหมายให้แก่ประเทศสมาชิก

---

[25] Council of Europe, The publications of The "European Treaty Series" and the explanatory reports. [online] Available from : http://www.europa.ru.int/treaty/html.

ดังนั้น หากพิจารณาถึงมาตรการทางกฎหมายของสหภาพยุโรปในการป้องกันและปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์นั้น ได้มีการวางมาตรการทางกฎหมายไว้ในบทบัญญัติแห่งกฎหรือคำสั่งต่างๆ แห่งธนาคารกลางยุโรป (European Central Bank Regulation and Division) ซึ่งมีสาระสำคัญดังนี้

3.1.3.1 คำสั่งแห่งธนาคารกลางยุโรปว่าด้วยการป้องกันการฉ้อโกง ณ วันที่ 7 ตุลาคม 2542 (Decision of the European Central Bank of 7 October 1999 on Fraud Prevention)

ธนาคารกลางยุโรปเป็นหน่วยงานหลักที่มีอำนาจหน้าที่ในการกำกับดูแลและควบคุมการให้บริการทางด้านการเงินการธนาคารภายในประเทศสมาชิกแห่งสหภาพยุโรป ดังนั้น ธนาคารกลางยุโรปได้กำหนดมาตรการทางกฎหมายในการทำหน้าที่ปกป้องและคุ้มครองระบบการเงินการธนาคารของประเทศสมาชิกแห่งสหภาพยุโรป ซึ่งเป็นไปตามข้อเสนอของคณะกรรมาธิการธนาคารกลางยุโรป ซึ่งได้มีความเห็นร่วมกันว่า ธนาคารกลางยุโรป สถาบันต่างๆ ทางการเงินการธนาคารของสหภาพยุโรป และประเทศสมาชิกต้องให้ความสำคัญกับการป้องกันการกระทำอันเป็นการฉ้อโกง ทุจริต การกระทำที่ผิดต่อกฎหมายและเป็นการกระทำที่มีผลกระทบต่อผลประโยชน์ใดๆ ทางการเงินการธนาคาร ซึ่งประเทศสมาชิกแห่งสหภาพยุโรปต้องร่วมกันต่อต้านการฉ้อโกงที่อาจเกิดขึ้นภายในประเทศสหภาพยุโรป โดยสาระสำคัญแห่งคำสั่งดังกล่าวมีดังนี้

3.1.3.1.1 ธนาคารกลางยุโรปกำหนดให้มีสำนักงานคณะกรรมาธิการตรวจสอบภายใน

ตามคำสั่งว่าด้วยการป้องกันการฉ้อโกง ณ วันที่ 7 ตุลาคม 2542 มาตรา 2 (Decision of the European Central Bank of 7 October 1999 on Fraud Prevention Article 2) [26] กำหนดให้คณะกรรมาธิการตรวจสอบภายใน (The Directorate for Internal Audit) เป็นผู้มีอำนาจหน้าที่การสืบสวนสอบสวน และรายงานถึงการใดๆ อันเป็นการฉ้อโกง หรือการกระทำอัน

---

[26] Decision of the European Central Bank of 7 October 1999 on Fraud Prevention, Article 2. [online] Available from :http://www.europa.eu.int/eurlex/en/lif/dat/1999/en_399DO726.html.

ผิดต่อกฎหมายเป็นอันตรายต่อระบบธนาคาร ซึ่งเป็นไปตามมาตรฐานและหรือประมวลกฎหมายแห่งธนาคารกลางยุโรป

3.1.3.1.2 สำนักงานคณะกรรมาธิการตรวจสอบภายในดังกล่าวมีอำนาจในการทำงานโดยอิสระ

ตามคำสั่งว่าด้วยการป้องกันการฉ้อโกง ณ วันที่ 7 ตุลาคม 2542 มาตรา 3 (Decision of the European Central Bank of 7 October 1999 on Fraud Prevention Article 3) ได้กำหนดให้สำนักงานคณะกรรมาธิการตรวจสอบภายในมีอำนาจสืบสวนสอบสวน รายงาน รวมทั้งออกคำสั่งใดๆที่เกี่ยวข้องกับการป้องกัน และตรวจสอบการฉ้อโกงหรือการกระทำอันผิดกฎหมายได้โดยอิสระและมิต้องถูกควบคุมจากหน่วยงานใด ๆ เพื่อให้สำนักงานคณะกรรมาธิการดังกล่าวสามารถทำงานได้อย่างมีประสิทธิภาพ[27]

3.1.3.1.3 คณะกรรมการต่อต้านการฉ้อโกงเป็นผู้ดำเนินงานภายในสำนักงานคณะกรรมาธิการตรวจสอบภายในของธนาคารกลางยุโรป

ตามคำสั่งว่าด้วยการป้องกันการฉ้อโกง ณ วันที่ 7 ตุลาคม 2542 มาตรา 1 (Decision of the European Central Bank of 7 October 1999 on Fraud Prevention Article 1) ได้กำหนดให้คุณสมบัติของคณะกรรมการต่อต้านการฉ้อโกงแห่งธนาคารกลางยุโรปที่แต่งตั้งขึ้น เพื่อให้เป็นผู้ทำหน้าที่ภายในสำนักงานคณะกรรมาธิการตรวจสอบภายในแห่งธนาคารกลางยุโรป และเป็นผู้สนับสนุนการทำงานของสำนักงานคณะกรรมาธิการตรวจสอบภายใน

---

[27] Decision of the European Central Bank of 7 October 1999 on Fraud Prevention , Article 3. [online] Available from :http://www.europa.ru.int/eurlex/en/lif/dat/1999/en_399DO726.html.

3.1.3.2 กฎแห่งธนาคารยุโรปที่ 2157/1999 ซึ่งกำหนดอำนาจหน้าที่ของธนาคารกลางยุโรป (European Central Bank Regulation (EC) No.2157/1999)

กฎแห่งธนาคารกลางยุโรปที่ 2157/1999 ว่าด้วยอำนาจแห่งธนาคารกลางยุโรป (European Central Bank Regulation (EC) No.2157/1999)[28] ซึ่งกำหนดถึงอำนาจหน้าที่ของธนาคารกลางยุโรปในการควบคุมและวางมาตรการต่างๆ ทางการเงินการธนาคารให้แก่ธนาคารของประเทศสมาชิกแห่งสหภาพยุโรป โดยให้คณะกรรมการแห่งธนาคารกลางยุโรปเป็นผู้มีอำนาจหน้าที่ในการกำหนดมาตรการ หรือบทกำหนดโทษภายใต้ กฎ คำสั่งต่างๆ แห่งสภาสหภาพยุโรป ทั้งนี้ อำนาจหน้าที่ของธนาคารกลางยุโรปในการป้องกัน และปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ มีสาระสำคัญสรุปได้ดังนี้

1. กำหนดมาตรการในการกำหนดบทลงโทษให้สถาบันต่างๆ ภายในประเทศสมาชิกต้องปฏิบัติกฎ คำสั่ง หรือระเบียบแห่งสภาสหภาพยุโรป
2. วางมาตรการในการปกป้องและจัดการกับการแลกเปลี่ยนข้อมูลทางธนาคารภายในระบบธนาคารกลางแห่งสหภาพยุโรป
3. กำหนดกฎเกณฑ์แก่ธนาคารกลางแห่งประเทศสมาชิกต่างๆ ของสหภาพยุโรปในการจัดการและรองรับต่อการกระทำการต่างๆ โดยผิดกฎหมายให้สามารถดำเนินการกับกระทำการดังกล่าวได้อย่างมีประสิทธิภาพ

โดยปกติแล้วการดำเนินการทางธนาคารถือว่าข้อมูลในการดำเนินการทางธนาคารจัดเป็นความลับทางธนาคาร ไม่ว่าจะเป็นข้อมูลทางบัญชี เอกสาร ตราสารที่เกี่ยวข้องกับการโอนเงิน ด้วยเหตุนี้จึงส่งผลให้อาชญากรรมที่เกิดขึ้นในการโอนเงินหรือการดำเนินงานทางธนาคารเป็นไปได้โดยสะดวก ดังนั้น ตามกฎว่าด้วยอำนาจหน้าที่แห่งธนาคารกลางยุโรปจึงกำหนดให้ธนาคารกลางยุโรปมีอำนาจและหน้าที่ในการกำหนดมาตรการในการจัดการกับข้อมูลทางบัญชีซึ่งถือเป็นความลับทางธนาคารดังกล่าวได้ในบางกรณี เพื่อป้องกันและปราบปรามอาชญากรรมที่เกิดขึ้นในกรณีดังกล่าว

---

[28] European Central Bank Regulation (EC) No. 2157/1999. [online] Available from : http://www.europa.eu.int/eurlex/en/lif/dat/1999/en_.html.

ดังนั้น จะเห็นได้ว่าธนาคารกลางยุโรปจึงเป็นหน่วยงานสำคัญในการวางมาตรการทางกฎหมายในการปราบปรามการอาชญากรรมทางระบบการเงินการธนาคารในภาพรวมให้แก่ประเทศสมาชิกของสหภาพยุโรป ซึ่งรวมถึงอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ด้วย เพื่อให้สามารถใช้บังคับได้กับประเทศสมาชิกแห่งสหภาพยุโรปได้

อย่างไรก็ตาม นอกเหนือจากมาตรการทางกฎหมายของสหภาพยุโรปในการป้องกันและปราบปรามการกระทำอันเป็นการฉ้อโกง หรือการกระทำทุจริตทางการเงินการธนาคารดังที่ได้อธิบายแล้วข้างต้นนั้น สหภาพยุโรปยังได้มีการวางมาตรการทางกฎหมายในการป้องกันและปราบปรามการใช้ระบบทางธนาคารเพื่อในการฟอกเงินอีกลักษณะหนึ่ง ซึ่งย่อมรวมถึงการโอนเงินเพื่อการฟอกหรือปกปิดที่มาของเงินดังกล่าว

3.1.3.3 คำแนะนำของคณะกรรมาธิการสหภาพยุโรป (Recommendation No. R (80) 10)

โดยคณะกรรมาธิการแห่งสหภาพยุโรป ได้กำหนดมาตรการในการป้องกันและปราบปรามอาชญากรรมต่อระบบธนาคารเพื่อการฟอกเงินไว้ในคำแนะนำที่ R (80) 10 ว่าด้วยมาตรการต่อต้านการโอนเงินและการปกปิดเงินที่ได้มาจาก หรือมีที่มาจากการกระทำความผิด (Measures against the transfer and safeguarding of funds of criminal origin, Recommendation No. R (80) 10) ซึ่งได้บัญญัติขึ้นเมื่อวันที่ 27 มิถุนายน ค.ศ.1980 โดยมีสาระสำคัญในการป้องกันและปราบปรามการฟอกเงินโดยการโอนเงิน ดังต่อไปนี้[29]

1. ธนาคารจะต้องมีบทบาทหรือวางมาตรการที่มีประสิทธิภาพในการป้องกันการโอนเงินเพื่อการฟอกเงิน หรือปกปิดที่มาของเงินดังกล่าว
2. พนักงานเจ้าหน้าที่ หรือพนักงานลูกจ้างของธนาคารต้องให้ความร่วมมือกับตำรวจ หรือผู้มีอำนาจหน้าที่ในการจัดการกับอาชญากรรมลักษณะดังกล่าว

---

[29] Banking for International Settlement. Prevention of Criminal Use of the Banking System for the purpose of Money-Laundering.(December 1988). [online] Available from : http://www.whitecase.com/bank_compliance.html.

3. ธนาคารจำเป็นต้องเปิดเผยข้อมูลอันเป็นความลับทางธนาคารบางประการเกี่ยวกับการกระทำความผิดดังกล่าว ทั้งนี้ เพื่อการสืบสวนสอบสวนและติดตามผู้กระทำความผิด

4. ธนาคารต้องจัดทำบันทึกรายการทางบัญชีที่มีข้อมูลทางบัญชีครบถ้วน เพื่อเป็นการสนับสนุนการจัดการหรือการดำเนินการทางธุรกิจเป็นไปอย่างมีประสิทธิภาพ และเป็นมาตรการสำคัญในการต่อต้านการฟอกเงินได้ในเบื้องต้น ประกอบกับ บันทึกรายการทางบัญชีต้องมีรายละเอียดต่อไปนี้

   4.1 วัตถุประสงค์ในการโอนเงิน

   4.2 ข้อมูลเฉพาะของลูกค้า เช่น ชื่อ ที่อยู่ รายละเอียดส่วนตัวของผู้โอนหรือผู้รับโอน

   4.3 บันทึกรายการทางบัญชีต้องเป็นไปตามรูปแบบมาตรฐาน

5. ผู้มีอำนาจหน้าที่ตามที่กฎหมายกำหนดต้องแสดงรายงานต่อคณะกรรมการกลางแห่งธนาคารกลางยุโรป

3.1.4 องค์การสหประชาชาติ (United Nation)

เนื่องจากองค์การสหประชาชาติโดยคณะกรรมาธิการสหประชาชาติว่าด้วยกฎหมายการค้าระหว่างประเทศ (UNCITRAL) ได้พิจารณาเห็นว่าควรมีการตรากฎหมายสากลว่าด้วยการโอนเงินระหว่างประเทศในการใช้เป็นมาตรฐาน และวางแนวทางร่วมกันสำหรับการควบคุมการโอนเงินหรือการโอนเครดิตระหว่างประเทศ เพื่อให้ประเทศต่างๆ ใช้ยึดถือเป็นแนวทางและหลักปฏิบัติสากล ด้วยเหตุนี้คณะกรรมาธิการสหประชาชาติ (UNCITRAL) จึงได้มีการตรากฎหมายแม่แบบว่าด้วยการโอนเงินระหว่างประเทศ (Model Law on International Credit Transfer)

3.1.4.1 กฎหมายแม่แบบว่าด้วยการโอนเงินระหว่างประเทศ (Model Law on International Credit Transfer)

โดยกฎหมายฉบับดังกล่าวมุ่งหมายให้ใช้บังคับครอบคลุมการโอนเงินทางอิเล็กทรอนิกส์ เกี่ยวกับความสมบูรณ์ ภาระหน้าที่ของแต่ละฝ่ายของการโอนเครดิตทางอิเล็กทรอนิกส์ และการโอนเงินโดยวิธีอื่นใดทุกประเภท แต่ หากพิจารณาถึงกฎหมายแม่แบบว่าด้วยการโอนเงินระหว่างประเทศดังกล่าวประกอบกับมาตรการทางกฎหมายดังกล่าวในการบังคับใช้กับอาชญากรรมคอมพิวเตอร์ในการโอนเงินทางอิเล็กทรอนิกส์ จะเห็นได้ว่า กฎหมาย

ฉบับดังกล่าวมิได้มีการบัญญัติถึงมาตรการในการป้องกันและปราบปรามหรือกำหนดลักษณะความผิดในการบังคับใช้กับการกระทำความผิด หรืออาชญากรรมทางคอมพิวเตอร์ที่เกิดขึ้นในการโอนเงินทางอิเล็กทรอนิกส์ไว้แต่อย่างใด เพียงแต่กำหนดถึงสิทธิ หน้าที่และความรับผิดของแต่ละฝ่ายที่เกี่ยวข้องกับการโอนเงินดังกล่าว และกำหนดมาตรการในการดำเนินการ การช่วยเหลือ หรือการแก้ไข หรือการดำเนินการใดๆ กรณีมีการโอนเงินที่มีข้อผิดพลาด ล่าช้า หรือล้มเหลวไว้เท่านั้น

แต่ในปัจจุบันอาชญากรรมที่เกิดขึ้นกับกระบวนการโอนเงินทางอิเล็กทรอนิกส์ได้มีการพัฒนาและเพิ่มจำนวนมากขึ้น ดังนั้น ที่ประชุมสมัชชาใหญ่แห่งองค์การสหประชาชาติจึงได้มีการออกมติที่ 55/188 ว่าด้วยการป้องกันและต่อต้านการประพฤติโดยมิชอบและโอนเงินโดยผิดกฎหมายและการปกปิดแหล่งที่มาของเงิน (Resolution 55/188 Preventing and combating corrupt practices and illegal transfer of funds and repatriation of such funds to the countries of origin)

3.1.4.2 มติที่ 55/188 ว่าด้วยการป้องกัน และต่อต้านการประพฤติโดยมิชอบและการโอนเงินโดยผิดกฎหมาย และปกปิดแหล่งที่มาของเงิน(Resolution 55/188 Preventing and combating corrupt practices and illegal transfer of funds and repatriation of such funds to the countries of origin)

มติที่ 55/188 เกี่ยวกับการป้องกันและต่อต้านการประพฤติโดยมิชอบและการโอนเงินโดยผิดกฎหมาย และปกปิดแหล่งที่มาของเงิน (Resolution 55/188 Preventing and combating corrupt practices and illegal transfer of funds and repatriation of such funds to the countries of origin)[30] ได้กำหนดมาตรการทางกฎหมายซึ่งเป็นหลักพื้นฐานในการป้องกันและต่อต้านการใช้ระบบธนาคารเป็นกระบวนการในการฟอกเงินหรือปิดบังที่มาหรือเงินที่ได้มาจากการกระทำความผิด ซึ่งมติดังกล่าวมีสาระสำคัญ กล่าวคือ

1. กำหนดมาตรการของการให้บริการธุรกิจ หรือสถาบันทางการเงิน การธนาคารของภาคเอกชนต้องปฏิบัติ โดยใช้หลักการปฏิบัติทางการเงินการธนาคาร ให้เป็นไปตามหลักธรรมเนียมประเพณี (Norm), ความซื่อสัตย์ (Honesty)

---

[30] General Assembly. Resolution adopted by the General Assembly 55/188. (Report of 87th Plenary Meeting, 20 December 2000) [online] Available from : http://www.uncitral.org.

2. กำหนดมาตรการในการใช้บังคับใช้กับการทุจริต การให้ผลประโยชน์ การฟอกเงิน และการโอนเงินผิดกฎหมาย
3. กำหนดมาตรการต่อต้านการกระทำทุจริตต่อการโอนเงิน และการสนับสนุนการทุจริตต่อการโอนเงินโดยทุจริตหรือผิดกฎหมาย
4. กำหนดมาตรการในการป้องกันการทุจริตการให้ผลประโยชน์ การฟอกเงิน และการโอนเงินผิดกฎหมาย
5. กำหนดให้มีมาตรการในการรายงานการโอนเงินในบางกรณี เพื่อตรวจสอบการโอนเงินว่าเข้าข่ายการโอนเงินโดยผิดกฎหมาย รวมถึงการตรวจสอบการโอนเงินเพื่อปกปิดหรือเปลี่ยนแปลงที่มาของเงินดังกล่าว
6. กำหนดให้มีมาตรการในการบังคับใช้หรือลงโทษในกรณีการโอนเงินโดยผิดกฎหมาย หรือการโอนเงินเพื่อปกปิดหรือเปลี่ยนแปลงที่มาของเงินดังกล่าว

3.2 มาตรการทางกฎหมายในการกำหนดลักษณะความผิดและบทกำหนดโทษแก่อาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

3.2.1 ประเทศสหรัฐอเมริกา (United State)

มาตรการทางกฎหมายในการกำหนดลักษณะความผิดและบทกำหนดโทษของความผิดที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ได้มีการบัญญัติไว้กฎหมายหลายฉบับดังที่ได้อธิบายไปแล้วข้างต้น ซึ่งหากพิจารณาถึงลักษณะของบทบัญญัติอันถือเป็นความผิดและบทกำหนดโทษของความผิดดังกล่าวตามกฎหมายแต่ละฉบับ จะเห็นได้ว่ากฎหมายแต่ละฉบับได้กำหนดลักษณะของการกระทำความผิด และบทกำหนดโทษของความผิดดังกล่าว ไว้เป็นการเฉพาะกล่าวคือ

3.2.1.1 พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ.1978

พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 (Electronic Fund Transfer Act,1978) ได้บัญญัติถึงการโอนเงินอันถือเป็นความผิดทางอาญาไว้ **กรณีการโอนเงินซึ่งเป็นการละเมิดการค้าระหว่างรัฐและการค้าระหว่างประเทศ ตามที่ได้บัญญัติไว้ในมาตรา 1693n (b) ว่าด้วยความรับผิดทางอาญา** ซึ่งมาตราดังกล่าวได้กำหนดการโอนเงินที่มีความผิดไว้หลายฐานความผิดซึ่งมีสาระสำคัญดังนี้

3.2.1.1.1 ความผิดต่อกระทำการทุจริตต่อบัตร, รหัส หรือสื่อทางอิเล็กทรอนิกส์

พระราชบัญญัติฉบับนี้ได้กำหนดความผิดอันเป็นการกระทำ ไม่ว่าจะเป็นการใช้ พยายาม หรือร่วมกันซึ่งทำการปลอม หลอกลวง เปลี่ยนแปลง ปลอมแปลง ทำลาย ทำให้สูญหาย โจรกรรม หรือการฉ้อโกงโดยวิธีใดๆ ต่อบัตรที่มีแถบแม่เหล็ก รหัสผ่าน หรือการเข้าถึงสื่ออิเล็กทรอนิกส์โดยวิธีหนึ่งวิธีใดในการโอนเงินทางอิเล็กทรอนิกส์ โดยเจตนาให้มีผลต่อการโอนเงินที่เกี่ยวข้องกับการค้าระหว่างรัฐหรือการค้าระหว่างประเทศ เพื่อให้ได้มาซึ่งเงิน สินค้า ค่าบริการ หรือสิ่งหนึ่งสิ่งใดที่มีมูลค่ารวมกันถึง1,000 ดอลลาร์สหรัฐ หรือมากกว่านั้นภายในระยะเวลา 1 ปี

3.2.1.1.2 ความผิดกระทำการทุจริต เพื่อให้ได้มาซึ่งบัตร รหัส หรือสื่อทางอิเล็กทรอนิกส์

พระราชบัญญัติฉบับนี้ได้กำหนดความผิด ไม่ว่าจะเป็นผู้ทำกระทำการพยายาม หรือร่วมกันกระทำการ ซึ่งเป็นการปลอม หลอกลวง เปลี่ยนแปลง ปลอมแปลง ทำลาย ทำให้สูญหาย โจรกรรม หรือฉ้อโกงโดยวิธีใด ๆ เพื่อให้ได้มาซึ่งบัตรที่มีแถบแม่เหล็ก รหัสผ่าน หรือการเข้าถึงสื่ออิเล็กทรอนิกส์โดยวิธีหนึ่งวิธีใดในการโอนเงินทางอิเล็กทรอนิกส์ โดยรู้ถึงการกระทำดังกล่าว เพื่อทำการทุจริตหรือฉ้อโกงการโอนเงินทางการค้าในประเทศและการค้าระหว่างประเทศ

3.2.1.1.3 ความผิดต่อการกระทำการทุจริต เพื่อให้ได้มาซึ่งบัตร รหัส หรือสื่อทางอิเล็กทรอนิกส์ และใช้บัตร รหัส หรือสื่อทางอิเล็กทรอนิกส์ที่ได้มาดังกล่าวโดยทุจริต

พระราชบัญญัติฉบับนี้ได้กำหนดความผิดในการปลอม หลอกลวง เปลี่ยนแปลง ปลอมแปลง ทำลาย ทำให้สูญหาย โจรกรรม หรือฉ้อโกงโดยวิธีใด ๆ เพื่อให้ได้มาซึ่งบัตรที่มีแถบแม่เหล็ก รหัสผ่าน หรือการเข้าถึงสื่ออิเล็กทรอนิกส์โดยวิธีหนึ่งวิธีใด เพื่อทำการขายหรือการโอนเงินทางการค้าในประเทศและการค้าระหว่างประเทศ โดยเจตนาทุจริตหรือฉ้อโกง การใช้บัตรที่มีแถบแม่เหล็ก รหัสผ่าน หรือการเข้าสื่ออิเล็กทรอนิกส์โดยวิธีหนึ่งวิธีใดในการโอนเงินทางอิเล็กทรอนิกส์ที่ได้มาดังกล่าว

3.2.1.1.4 การกระทำทุจริตต่อบัตร รหัส หรือสื่อทางอิเล็กทรอนิกส์ใดๆ เพื่อการได้รับ ปกปิด ใช้ หรือโอนเงิน ค่าสินค้าหรือค่าบริการ โดยการโอนเงินขององค์การระหว่างรัฐ หรือองค์การค้าระหว่างประเทศ

พระราชบัญญัติฉบับนี้ ได้กำหนดความผิดต่อการปลอม หลอกลวง เปลี่ยนแปลง ปลอมแปลง ทำลาย ทำให้สูญหาย โจรกรรม หรือฉ้อโกงโดยวิธีใด ๆ ต่อบัตรที่มีแถบแม่เหล็ก รหัสผ่าน หรือการเข้าถึงสื่ออิเล็กทรอนิกส์โดยวิธีหนึ่งวิธีใด เพื่อให้ได้รับมา การปกปิด การใช้ หรือการโอนซึ่งเงิน ค่าสินค้า ค่าบริการ หรือสิ่งหนึ่งสิ่งใดที่มีมูลค่า (ยกเว้นตราสารในการโอนเงินระหว่างรัฐหรือระหว่างประเทศ) เพื่อการโอนเงินขององค์การระหว่างรัฐ หรือองค์การค้าระหว่างประเทศ โดยภายในหนึ่งปีมีมูลค่ารวมกันถึง 1,000 ดอลลาร์สหรัฐหรือมากกว่านั้น

3.2.1.1.5 การกระทำทุจริตต่อบัตร รหัส หรือสื่อทางอิเล็กทรอนิกส์ใดๆ ในการได้รับไป การปกปิด การใช้ การขาย หรือการขนส่งตราสารในทางการค้าระหว่างประเทศ เพื่อให้ได้มาซึ่งสินค้าที่เช่าซื้อไว้

พระราชบัญญัติฉบับนี้ได้กำหนดความผิดต่อในการปลอม หลอกลวง เปลี่ยนแปลง ปลอมแปลง ทำลาย ทำให้สูญหาย โจรกรรม หรือการฉ้อโกงโดยวิธีหนึ่งวิธีใดต่อ

บัตรที่มีแถบแม่เหล็ก รหัสผ่าน หรือการเข้าถึงสื่ออิเล็กทรอนิกส์โดยวิธีหนึ่งวิธีใด เพื่อให้ได้มาการได้เช่าซื้อไว้ หรือได้รับมาซึ่งสิ่งหนึ่งสิ่งใดหรือมากกว่านั้น โดยการได้รับ การปกปิด การใช้ การขาย หรือการขนส่งตราสารหนึ่งๆ หรือมากกว่านั้นในทางการค้าระหว่างรัฐหรือการค้าระหว่างประเทศเพื่อทำการขนส่งในทางการค้าระหว่างรัฐหรือการค้าระหว่างประเทศภายในหนึ่งปี มีมูลค่ารวมกันถึง 500 ดอลลาร์สหรัฐขึ้นไป หรือมากกว่านั้น

3.2.1.1.6 ความผิดต่อการกระทำอันทำให้เกิดการเปลี่ยนแปลงทางบัญชีที่มีผลกระทบต่อการค้าระหว่างรัฐ หรือการค้าระหว่างประเทศ

พระราชบัญญัติฉบับนี้ได้กำหนดความผิดต่อการปลอม หลอกลวง เปลี่ยนแปลง ปลอมแปลง ทำลาย ทำให้สูญหาย โจรกรรม เพื่อที่ได้มาซึ่งเครื่องมือในการชำระหนี้ และรู้ถึงการปลอม หลอกลวง เปลี่ยนแปลง ปลอมแปลง ทำลาย ทำให้สูญหาย โจรกรรมหรือการฉ้อโกงโดยวิธีหนึ่งวิธีใด เพื่อให้เกิดการเปลี่ยนแปลงทางบัญชีที่มีผลกระทบต่อการค้าระหว่างรัฐ หรือการค้า หรือการค้าระหว่างประเทศ และสามารถจัดหาเงิน ทรัพย์สิน การบริการ หรือสิ่งหนึ่งสิ่งใดๆ ที่มีมูลค่าภายในหนึ่งปีและมีมูลค่ารวมกันถึง1,000 ดอลลาร์สหรัฐหรือมากกว่านั้น

<u>บทกำหนดโทษ</u>

ผู้ใดกระทำความผิดตั้งแต่ข้อ 3.2.1.1.1 – 3.2.1.1.6 ผู้นั้นมีโทษปรับไม่เกิน 10,000 ดอลลาร์สหรัฐ หรือจำคุกไม่เกินสิบปี หรือทั้งจำทั้งปรับ

3.2.1.2 ประมวลกฎหมายอาญา (FEDERAL CRIME AND CRIMINAL PROCEDURE)

ประเทศสหรัฐอเมริกาได้มีการบัญญัติกฎหมายที่บังคับใช้กับการอาชญากรรมประเภทต่าง ๆ ไว้ในประมวลกฎหมายอาญาแห่งประเทศสหรัฐอเมริกาโดยเฉพาะ ซึ่งบัญญัติไว้ในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 ว่าด้วยการกระทำความผิดทางอาญาและวิธีพิจารณาทางอาญา (United State Code, Title 18 - Crimes and Criminal Procedure) โดยประมวลกฎหมายอาญาดังกล่าวได้บัญญัติถึงการกระทำอันเป็นความผิดลักษณะต่าง ๆ ซึ่งแบ่งออกได้เป็น 6 ภาค ดังนี้

ภาค 1	การกระทำความผิดทางอาญา
ภาค 2	วิธีพิจารณาความอาญา
ภาค 3	สถานที่คุมขังและนักโทษ
ภาค 4	ผู้กระทำความผิดที่เป็นผู้เยาว์
ภาค 5	เอกสิทธิ์ของพยาน

จากการศึกษาจะเห็นได้ว่า บทบัญญัติภาค 1 เป็นบทบัญญัติที่ใช้บังคับกับความผิดในลักษณะต่างๆ ที่มีการบัญญัติถึงลักษณะของการกระทำความผิดและกำหนดโทษไว้ ซึ่งบทบัญญัติแห่งภาค 1 แบ่งออกตามลักษณะความผิดในหมวดต่างๆ ได้ตั้งแต่หมวด 1-123 โดยมีรายละเอียดดังต่อไปนี้

หมวด 1 ว่าด้วยบทบัญญัติที่ใช้บังคับแก่ความผิดโดยทั่วไป ซึ่งกำหนดถึงหลักกฎหมายทั่วไปทางอาญา ผู้สมรู้ร่วมคิด การตูหมิ่น บทนิยาม กฎหมายแห่งรัฐที่บังคับใช้เฉพาะพื้นที่ภายในเขตอำนาจแห่งรัฐบาลกลาง ภาระหน้าที่ของการรักษาความปลอดภัยของรัฐบาลต่างประเทศ ความผิดลหุโทษ หรือการกระทำโดยผู้วิกลจริต

หมวด 2-123 ว่าด้วยความผิดในแต่ละลักษณะความผิดยกตัวอย่างเช่น ความผิดต่อรัฐความผิดต่อชีวิต ความผิดต่อร่างกาย ความผิดต่อทางการเงินการธนาคาร ความผิดต่อทรัพย์สิน ความผิดต่อการกระทำของพนักงานเจ้าหน้าที่ ความผิดต่อชื่อเสียง ความผิดต่อเสรีภาพ เป็นต้น

ซึ่ง ประมวลกฎหมายอาญาได้กำหนดขอบเขตในการบังคับใช้กฎหมายภายใต้บทบัญญัติฉบับนี้ โดยได้กำหนดวัตถุประสงค์ในการบังคับใช้กฎหมายฉบับนี้ไว้ ตามมาตรา 2 กล่าวคือ

1. บุคคลใดที่กระทำความผิด ช่วยเหลือ สนับสนุน วางแผน ใช้ ชักจูง แนะนำ หรือก่อให้เกิดซึ่งการกระทำความผิดตามที่ได้บัญญัติ และกำหนดโทษไว้ตามบทบัญญัตินี้ในประเทศสหรัฐอเมริกา
2. บุคคลใดซึ่งมีเจตนาในการกระทำอันเป็นเหตุให้เกิดความผิดขึ้น หากกระทำนั้นเป็นการกระทำโดยตรง โดยบุคคลนั้นหรือบุคคลอีกคนหนึ่ง

ซึ่งอาจจะเป็นความผิดต่อประเทศสหรัฐอเมริกา ซึ่งเป็นการกระทำความผิด ตามที่ได้บัญญัติและกำหนดโทษไว้ตามบทบัญญัตินี้"[31]

ขอบเขตในการบังคับใช้ประมวลกฎหมายอาญาที่กำหนดไว้ข้างต้นจะเห็นได้ว่า ประมวลกฎหมายอาญาแห่งสหรัฐอเมริกามุ่งบังคับใช้กับความผิดที่เกิดขึ้น ณ ประเทศสหรัฐอเมริกาและบทบัญญัติฉบับนี้ได้กำหนดไว้ให้การกระทำดังกล่าวเป็นความผิดและกำหนดโทษไว้ ดังนั้น หากพิจารณาถึงมาตรการในการกำหนดลักษณะความผิดและบทกำหนดโทษอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญาฉบับนี้นั้น มีสาระสำคัญ ดังนี้

3.2.1.2.1 ความผิดในการทุจริตต่อตำแหน่งหน้าที่

ประมวลกฎหมายอาญานี้ ได้กำหนดลักษณะของความผิดเกี่ยวกับผู้ที่มีอำนาจหน้าที่เกี่ยวกับระบบการเงินการธนาคารและได้กระทำการให้ประโยชน์ หรือการรับประโยชน์เพื่อให้ทำการโอนเงินทางอิเล็กทรอนิกส์โดยการทุจริต หรือการทุจริตโดยพนักงานเจ้าหน้าที่หรือผู้มีอำนาจหน้าที่ของธนาคาร สถาบันทางการเงิน ธนาคารรัฐบาลกลาง หรือหน่วยงานของธนาคารรัฐบาลกลาง โดยมีรายละเอียดของความผิดในลักษณะความผิดดังกล่าวดังนี้

1. **ความผิดต่อการให้ รับประโยชน์อย่างหนึ่งอย่างใดในการโอนเงินทางอิเล็กทรอนิกส์**

ความผิดต่อ การกระทำใดๆ ในการ ใช้อิทธิพลอย่างหนึ่งอย่างใด หรือให้ประโยชน์แก่พนักงานเจ้าหน้าที่หรือผู้ที่มีส่วนเกี่ยวข้องหรือผู้ที่มีอำนาจหน้าที่ในการโอนเงินหรือการรับประโยชน์ของพนักงานเจ้าหน้าที่หรือผู้ที่มีส่วนเกี่ยวข้อง เพื่อการโอนเงินของสถาบันการเงิน และให้ได้มาซึ่งเงินหรือประโยชน์อย่างหนึ่งอย่างใดนั้น โดยความผิดดังกล่าวได้บัญญัติไว้ในมาตรา 215[32] และมีสาระสำคัญขององค์ประกอบความผิด ดังนี้

1. ผู้ใดโดยเจตนาทุจริตในการใช้อิทธิพลหรือให้สิ่งตอบแทนแก่ เพื่อให้ได้มา, เสนอ หรือให้สัญญาที่มีมูลค่าอย่างหนึ่งอย่างใดให้

---

[31] United State Code,(Title 18 : Crimes and Criminal Procedure, section 2.). [online] Available from : http://caselaw.lp.findlaw.com.

[32] Ibid., section 215.

แก่พนักงานเจ้าหน้าที่ กรรมการ ลูกจ้าง ตัวแทน หรือผู้รับมอบอำนาจของสถาบันทางการเงินในการดำเนินธุรกิจหรือการโอนเงินของนิติบุคคลนั้น

2. ผู้ใดเป็นพนักงานเจ้าหน้าที่ กรรมการ ลูกจ้าง ตัวแทน หรือผู้รับมอบอำนาจของสถาบันทางการเงิน ซึ่งเป็นผู้ชักชวนและต้องการซึ่งประโยชน์อย่างหนึ่งอย่างใด หรือยอมรับหรือเห็นชอบในการยอมรับ ซึ่งประโยชน์อย่างหนึ่งอย่างใดจากบุคคลหนึ่งบุคคลใดโดยทุจริต และจงใจใช้อิทธิพลหรือให้สิ่งตอบแทนเพื่อการดำเนินธุรกิจหรือการโอนเงินของสถาบันทางการเงินนั้น

<u>บทกำหนดโทษ</u>

1. ผู้นั้นมีโทษปรับไม่เกิน 1,000,000 ดอลลาร์ หรือสามเท่าของมูลค่าซึ่งสิ่งที่ให้ เสนอ สัญญา ชักชวน เรียกร้อง ยอมรับ หรือเห็นควรในการยอมรับ หรือสิ่งหนึ่งสิ่งใดที่มีมูลค่ามากกว่านั้น หรือ มีโทษจำคุกไม่เกิน สามสิบ ปี หรือทั้งจำทั้งปรับ ทั้งนี้หากมูลค่าซึ่งสิ่งที่ให้ เสนอ สัญญา ชักชวน เรียกร้อง ยอมรับ หรือเห็นควรในการยอมรับนั้นมีมูลค่าไม่เกิน 1,000 ดอลลาร์ ผู้นั้นมีโทษปรับเป็นไปตามที่กำหนดไว้ในบทบัญญัติฉบับนี้ หรือมีโทษจำคุกไม่เกิน หนึ่ง ปี หรือทั้งจำทั้งปรับ
2. ความผิดดังกล่าวอยู่ภายใต้การบังคับใช้ของมาตรการริบทรัพย์สินตามมาตรา 981 และมาตรา 982 แห่งประมวลกฎหมายฉบับนี้ ซึ่งจะได้อธิบายในรายละเอียดต่อไป

2. ความผิดต่อทุจริตโดยผู้ตรวจสอบธนาคาร หรือผู้ตรวจสอบสถาบันทางการเงิน

ความผิดต่อการทุจริตของผู้ตรวจสอบธนาคารหรือผู้ตรวจสอบสถาบันทางการเงิน ตามมาตรา 655 ได้กำหนดถึง การกระทำความผิดของผู้ตรวจสอบธนาคาร หรือผู้ตรวจสอบสถาบันการเงินซึ่งได้ทำการโดยวิธีหนึ่งวิธีใดที่กำหนดไว้ในมาตรานี้ ไม่ว่าจะเป็น การขโมย การปกปิด การซ่อนเร้น หรือการกระทำการใดๆ เพื่อให้ได้มาซึ่งเงิน เครดิต หรือ

มาตรการความปลอดภัยของทรัพย์สินหรือสิ่งหนึ่งสิ่งใดของธนาคารไว้โดยเฉพาะ โดยอาศัยอำนาจหน้าที่ของตนที่มีภายในระบบการเงินการธนาคารทำการใดๆ ดังกล่าว

ซึ่งหากพิจารณาถึง องค์ประกอบความผิดของการลักทรัพย์โดยผู้ตรวจสอบของธนาคารหรือสถาบันทางการเงินตามมาตรา655[33] กล่าวคือ

1. ผู้ใดซึ่งเป็นผู้ตรวจสอบของธนาคารหรือสถาบันทางการเงินหรือผู้ช่วยผู้ตรวจสอบดังกล่าว
2. ขโมย หรือทำการใดๆ โดยผิดต่อกฎหมาย หรือการปกปิดหรือซ่อนเร้นโดยผิดต่อกฎหมาย เพื่อให้ได้มาซึ่งเงิน เครื่องหมายดร๊าฟท์ สัญญา หรือมาตรการความปลอดภัย หรือทรัพย์สินสิ่งหนึ่งสิ่งใดที่มีมูลค่าอย่างหนึ่งอย่างใดที่อยู่ในการครอบครองของธนาคารหรือสถาบันทางการเงินต่อไปนี้
   2.1 ธนาคารหรือสถาบันทางการเงิน
   2.2 สถาบันทางการเงินซึ่งเป็นสมาชิกของระบบธนาคารรัฐบาลกลาง และอยู่ในการประกันของบริษัทประกันภัยเงินฝากของธนาคารรัฐบาลกลาง
   2.3 ธนาคารสาขาหรือตัวแทนของธนาคารต่างประเทศ
   2.4 นิติบุคคลที่ดำเนินกิจการธนาคารและได้รับการอนุญาตตามมาตรา 25 แห่งพระราชบัญญัติธนาคารรัฐบาลกลาง (Federal Reserve Act)
   2.5 มาตรการความปลอดภัยของตู้เงินฝากที่อยู่ในธนาคาร หรือตู้เงินฝากที่เชื่อมต่อและถือเป็นส่วนหนึ่งของธนาคาร ธนาคารสาขา ธนาคารตัวแทน หรือนิติบุคคลที่ดำนินกิจการธนาคาร

<u>บทกำหนดโทษ</u>

ผู้นั้นมีโทษปรับภายใต้พระราชบัญญัติฉบับนี้ หรือ มีโทษจำคุกไม่เกินห้าปี หรือทั้งจำทั้งปรับ และผู้นั้นต้องถูกตัดสิทธิในการเป็นผู้ตรวจสอบที่ลงทะเบียนไว้ ณ

---

[33] United State Code,(Title 18 : Crimes and Criminal Procedure, section 655). [online] Available from : http://caselaw.lp.findlaw.com.

ธนาคารแห่งชาติ หรือบริษัทประกันภัยเงินฝากของธนาคารรัฐบาลกลาง แต่ถ้าเงินที่ให้ได้มาหรือปกปิดหรือซ่อนเร้นมีมูลค่าไม่มากกว่า 1,000 ดอลลาร์สหรัฐ ผู้นั้นมีโทษปรับเป็นไปตามที่กำหนดไว้ในบทบัญญัติฉบับนี้ หรือมีโทษจำคุกไม่เกิน หนึ่ง ปี หรือทั้งจำทั้งปรับและผู้นั้นต้องถูกตัดสิทธิในการเป็นผู้ตรวจสอบที่ลงทะเบียนไว้ ณ ธนาคารแห่งชาติ หรือบริษัทประกันภัยเงินฝากของธนาคารรัฐบาลกลาง

3. ความผิดต่อการทุจริตของพนักงานเจ้าหน้าที่ธนาคารหรือสถาบันทางการเงิน

ความผิดต่อทุจริตของพนักงานเจ้าหน้าที่ธนาคาร หรือสถาบันทางการเงิน ไม่ว่าจะเป็นการลักทรัพย์ การยักยอก หรือการกระทำโดยให้ข้อมูลที่ไม่ถูกต้องทางการธนาคาร โดยพนักงานเจ้าหน้าที่ธนาคารหรือสถาบันทางการเงินต่างๆ เพื่อให้ได้มาซึ่งเงิน หรือประโยชน์อื่นใดของธนาคารหรือสถาบันทางการเงิน ซึ่งได้บัญญัติไว้ในมาตรา 656 และมาตรา 657 แห่งประมวลกฎหมายอาญานี้ โดยลักษณะของการกระทำดังกล่าว เป็นการอาศัยอำนาจหน้าที่ที่มีอยู่ระบบการเงินการธนาคารของตน ซึ่งเป็นพนักงาน หรือเจ้าหน้าที่ธนาคารหรือสถาบันทางการเงินกระทำการอย่างหนึ่งอย่างใด เพื่อให้ได้มา ซึ่งเงิน เครดิต หรือมาตรการความปลอดภัย ทรัพย์

หากพิจารณาถึงองค์ประกอบความผิดของการลักทรัพย์ การยักยอก หรือการให้ข้อมูลที่ไม่ถูกต้องทางการธนาคาร โดยพนักงานเจ้าหน้าที่หรือลูกจ้างของธนาคาร หรือสถาบันที่เกี่ยวข้องกับระบบการเงินการธนาคารตามมาตรา656[34] และมาตรา 657[35] นี้ ซึ่งบทบัญญัติดังกล่าวมีองค์ประกอบความผิด ดังนี้

1. ผู้ใดซึ่งเป็นพนักงานเจ้าหน้าที่ กรรมการ ตัวแทน พนักงาน ลูกจ้างธนาคาร หรือสถาบันทางการเงินต่างๆ ตัวแทนหรือผู้ที่ได้รับมอบหมายให้ติดต่อกับธนาคาร หรือสถาบันต่างๆ ที่เกี่ยวข้องกับระบบการเงินการธนาคาร ดังต่อไปนี้

1.1 มาตรา 656 ได้กำหนดถึงสถาบันที่เกี่ยวข้องกับระบบการเงินการธนาคาร ตามที่ได้กำหนดไว้ ดังนี้

1.1.1 ธนาคารที่ได้รับอนุญาตจากธนาคารรัฐบาลกลาง

---

[34] United State Code,(Title 18 : Crimes and Criminal Procedure, section 656). [online] Available from : http://caselaw.lp.findlaw.com.

[35] Ibid., section 657.

1.1.2 ธนาคารสมาชิก

1.1.3 สถาบันรับฝากเงินที่ถือหุ้นโดยบริษัท

1.1.4 ธนาคารแห่งชาติ

1.1.5 ธนาคารที่ได้รับการรับรอง

1.1.6 ธนาคารสาขาหรือธนาคารตัวแทนของธนาคารต่างประเทศ

1.1.7 นิติบุคคลใดที่ดำเนินกิจการธนาคารและได้รับการอนุญาตตามมาตรา 25 แห่งพระราชบัญญัติธนาคารรัฐบาลกลาง (Federal Reserve Act)

1.1.8 สถาบันที่ได้รับอนุญาตจากธนาคารแห่งชาติหรือธนาคารที่ได้รับการรับรอง

1.1.9 ธนาคารสาขา หรือธนาคารตัวแทน หรือนิติบุคคล หรือตัวแทน หรือลูกจ้างของผู้รับเงินนั้น หรือองค์กรที่ทำหน้าที่แทนระบบธนาคารรัฐบาลกลาง

1.2 มาตรา 657 ได้กำหนดถึงสถาบันที่เกี่ยวข้องกับระบบการเงินการธนาคาร ซึ่งเป็นสถาบันทางการเงินการธนาคารที่นอกเหนือไปจากที่กำหนดไว้ในมาตรา 656 ดังนี้

1.2.1 บริษัทประกันภัยเงินฝากของรัฐบาลกลาง

1.2.2 กลุ่มสหกรณ์เงินกู้แห่งชาติ

1.2.3 สำนักงานตรวจตราการออมทรัพย์แห่งชาติ

1.2.4 บริษัทสินเชื่อหรือทรัสต์

1.2.5 ธนาคารสินเชื่อที่อยู่อาศัย

1.2.6 คณะกรรมการรัฐบาลกลางของธนาคารเพื่อการเคหะ

1.2.7 ธนาคารสินเชื่อเพื่อการเกษตร

1.2.8 องค์กรพัฒนาเคหะหรือชุมชนชานเมือง

1.2.9 สถาบันประกันข้าวโพด

1.2.10 บริษัทที่ให้กู้ยืม รับฝากเงิน ประกันภัย ให้เครดิตหรือออมทรัพย์

1.2.11 นิติบุคคลที่อยู่ภายใต้การควบคุมของสถาบันต่างๆ ภายในประเทศสหรัฐอเมริกานอกเหนือไปจากมาตรา 656

1.2.12 สถาบันที่ได้รับการรับรองโดยบริษัทประกันเงินฝากของรัฐบาลกลาง

1.2.13 คณะกรรมการแห่งสหกรณ์เงินกู้แห่งประเทศสหรัฐอเมริกา

1.2.14 บริษัทลงทุนรายย่อย

1.2.15 สถาบันพัฒนาทางการธนาคารชุมชน

2. ยักยอก หลอกลวง ลัก หรือให้ข้อมูลทางธนาคารที่ไม่ถูกต้อง

3. เพื่อให้ได้มาซึ่งเงิน หรือเงินฝาก หรือทรัพย์สิน หรือมาตรการความปลอดภัยที่ใช้ควบคุมธนาคารหรือสถาบันต่างๆ ข้างต้น หรือมาตรการเพื่อควบคุมกำกับดูแลตัวแทน พนักงานเจ้าหน้าที่ หรือพนักงานลูกจ้างของสถาบันต่างๆ ข้างต้น

บทลงโทษ

1. ผู้นั้นมีโทษปรับไม่เกิน 1,000,000 ดอลลาร์สหรัฐ หรือมีโทษจำคุกไม่เกิน สามสิบ ปี หรือทั้งจำทั้งปรับ แต่หากการกระทำดังกล่าวมีมูลค่าไม่มากกว่า 1,000 ดอลลาร์สหรัฐ ผู้นั้นมีโทษปรับเป็นไปตามที่กำหนดไว้ในบทบัญญัติฉบับนี้ หรือมีโทษจำคุกไม่เกิน หนึ่ง ปี หรือทั้งจำทั้งปรับ

2. ความผิดดังกล่าวอยู่ภายใต้การบังคับใช้ของมาตรการริบทรัพย์สินตามมาตรา 981 และมาตรา 982 แห่งประมวลกฎหมายฉบับนี้ ซึ่งจะได้อธิบายในรายละเอียดต่อไป

4. ความผิดต่อการทุจริตของผู้มีอำนาจหน้าที่เกี่ยวข้องกับระบบการเงินการธนาคารแห่งรัฐบาลกลาง

ความผิดอันเป็นการกระทำทุจริตของผู้ที่มีอำนาจหน้าที่ที่เกี่ยวข้องกับระบบการเงินการธนาคารแห่งรัฐบาลกลางได้กำหนดไว้ในประมวลกฎหมายสหรัฐอเมริกา ตามมาตรา 666 ซึ่งความผิดลักษณะดังกล่าวเป็นความผิดที่ต้องอาศัยอำนาจหน้าที่ของผู้ที่เกี่ยวข้องกับ

ระบบการเงินการธนาคาร และผู้กระทำการใดๆ เพื่อให้มาซึ่งการโอนเงินภายใต้ระบบการเงินการธนาคาร ซึ่งความผิดลักษณะดังกล่าวจึงเป็นความผิดที่เกิดขึ้นภายใต้ระบบการโอนเงินทางอิเล็กทรอนิกส์ ดังนั้นความผิดดังกล่าวจึงถือเป็นอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์เช่นเดียวกัน

หากพิจารณาถึงลักษณะความผิดตามมาตรา 666[36] มีองค์ประกอบความผิดดังนี้

1. ผู้นั้นเป็นตัวแทนของนิติบุคคลหรือรัฐ รัฐบาลแห่งรัฐ รัฐบาลท้องถิ่น หรือตัวแทนของรัฐบาลดังกล่าว กระทำการชักชวน หรือจัดหาเพื่อให้ได้มาซึ่งประโยชน์อย่างหนึ่งอย่างใดแก่บุคคลหนึ่ง หรือยอมรับหรือตกลงในการยอมรับในสิ่งหนึ่งสิ่งใดจากบุคคลหนึ่งโดยทุจริต และจงใจใช้อิทธิพลหรือให้สิ่งตอบแทนใด ๆ เพื่อการติดต่อธุรกิจ การโอนเงิน หรือการทำธุรกรรมใดๆ ในการโอนเงินของนิติบุคคล ของรัฐบาล หรือตัวแทนนิติบุคคลนั้นที่รวมกันมีมูลค่าถึง 5,000 ดอลลาร์สหรัฐ หรือมากกว่านั้น
2. บุคคลใดทำการทุจริตโดยในการให้ เสนอ หรือตกลงให้สิ่งหนึ่งสิ่งใดที่มูลค่าแก่บุคคลหนึ่งบุคคลใด โดยจงใจใช้อิทธิพลหรือให้สิ่งตอบแทนใดๆ แก่ตัวแทนรัฐบาล ตัวแทนนิติบุคคลอื่นๆ หรือองค์กรของรัฐที่ได้กล่าวมาแล้ว เพื่อการติดต่อธุรกิจ การโอนเงิน หรือการทำธุรกรรมใดๆ ในการโอนเงินของนิติบุคคล ของรัฐบาล หรือตัวแทนที่รวมกันมีมูลค่าถึง 5,000 ดอลลาร์สหรัฐ หรือมากกว่านั้น
3. กรณีข้างต้นเป็นการกระทำโดยการใช้ระบบหรือโปรแกรมของธนาคารรัฐบาลกลางในการทำโอนทางการเงินดังกล่าว ซึ่งมีมูลค่าของเงินหรือผลประโยชน์ดังกล่าวภายในระยะเวลา หนึ่ง ปี มีมูลค่าเกินกว่า 10,000 ดอลลาร์สหรัฐ

---

[36] United State Code, (Title 18 : Crimes and Criminal Procedure, section 666). [online] Available from : http://caselaw.lp.findlaw.com.

บทลงโทษ

ผู้นั้นมีโทษปรับเป็นไปตามที่กำหนดไว้ในบทบัญญัติฉบับนี้ หรือมีโทษจำคุกไม่เกิน สิบ ปี หรือทั้งจำทั้งปรับ

3.2.1.2.2 ความผิดต่อการฉ้อโกงทางการเงินการธนาคาร

ประมวลกฎหมายอาญานี้ได้กำหนดลักษณะความผิดฐานฉ้อโกงในลักษณะต่างๆ ที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ไว้ในหลายลักษณะความผิด กล่าวคือ

1. ความผิดต่อการฉ้อโกงบันทึก รายงานหรือการเปลี่ยนแปลงทางบัญชี

ความผิดต่อการฉ้อโกงบันทึก รายงานหรือการเปลี่ยนแปลงทางบัญชีของสถาบันที่เกี่ยวข้องกับระบบการเงินการธนาคารต่างๆ ได้บัญญัติไว้ในหมวดที่ 47 ว่าด้วยการฉ้อโกงและแสดงรายการทางบัญชีที่ไม่ถูกต้อง ภายใต้บทบัญญัติแห่งมาตรา 1005 มาตรา 1006 และมาตรา 1007 ซึ่งความผิดแต่ละมาตราดังกล่าวมีองค์ประกอบในการกระทำความผิดเกี่ยวกับการฉ้อโกงบันทึก รายงาน และการเปลี่ยนแปลงรายการทางบัญชีที่แตกต่างกันตามแต่ละลักษณะความผิด หรือสถาบันทางการเงิน ซึ่งหากพิจารณาถึงความผิดเกี่ยวกับบันทึก รายงานและรายการทางบัญชีในการโอนเงินทางอิเล็กทรอนิกส์โดยทั่วไปอยู่ภายใต้การควบคุม กำกับ และดูแลตามบทบัญญัติแห่งพระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ซึ่งได้กำหนดความรับผิดทางอาญาในการแจ้งข้อความอันเป็นเท็จ หรือข้อความที่ไม่ถูกต้องต่อความจริง หรือข้อมูลที่ต้องเปิดเผยในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

ซึ่งหากพิจารณาบทบัญญัติในมาตรา 1005 มาตรา 1006 และมาตรา 1007 นี้แล้วจะเห็นว่า บทบัญญัติดังกล่าวเป็นการกำหนดลักษณะความผิดและบทกำหนดโทษเพิ่มเติมจากความผิดในพระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ในกรณีการแจ้งข้อความอันเป็นเท็จหรือข้อมูลที่ไม่ถูกตรงกับความจริงเกี่ยวกับบันทึก รายงาน หรือการเปลี่ยนแปลงทางบัญชีของธนาคาร หรือสถาบันทางการเงิน และสร้างความเสียหายให้แก่ธนาคารหรือสถาบันทางการเงิน หรือเป็นการเพื่อหลอกลวงเจ้าหน้าที่

องค์ประกอบความผิดตามมาตรา 1005 [37] มีรายละเอียดดังนี้

1. ผู้ใดซึ่งเป็นพนักงานเจ้าหน้าที่ กรรมการ ตัวแทน ลูกจ้างของสถาบันทางการเงินตามมาตรานี้ทำการออกบันทึกอันเป็นที่ยอมรับทางธนาคาร โดยปราศจากอำนาจจากกรรมการธนาคาร หรือสถาบันทางการเงินดังกล่าว
2. ผู้ใด ซึ่งปราศจากอำนาจในการจัดการ การเพิกถอน ดำเนินการใดๆ ในการรับรองคำสั่งทางธนาคารหรือสถาบันทางการเงิน
3. ผู้ใด ซึ่งทำการใส่ข้อมูลที่ไม่ถูกต้องในสมุดบัญชีธนาคาร รายงาน และ รายการทางบัญชีของสถาบันทางการเงินการธนาคาร โดยเจตนาฉ้อโกง หรือมุ่งสร้างความเสียหายแก่สถาบันทางการเงินการธนาคารดังกล่าว นิติบุคคลใดๆ บริษัท ประชาชน หรือบุคคลธรรมดา หรือเพื่อหลอกลวงพนักงานเจ้าหน้าที่แห่งสถาบันทางการเงินการธนาคารนั้นๆ หรือผู้ตรวจสอบที่มีอำนาจหน้าที่ในการตรวจสอบสถาบันทางการเงินการธนาคารดังกล่าว
4. ผู้ใดเจตนาฉ้อโกงต่อประเทศสหรัฐอเมริกา ตัวแทน หรือสถาบันทางการเงิน ทั้งนี้รวมถึงผู้ที่ได้รับเงิน ผลประโยชน์ ทรัพย์สิน ผลกำไรผ่านการโอนทางบัญชี ไม่ว่าทางตรงหรือทางอ้อม หรือผู้ที่มีส่วนร่วมในการกระทำความผิด
5. สถาบันทางการเงินการธนาคารตามมาตรานี้ ได้แก่
   - 5.1 ธนาคารรัฐบาลกลาง
   - 5.2 ธนาคารสมาชิก
   - 5.3 สถาบันเงินฝากที่ถือหุ้นโดยบริษัท
   - 5.4 ธนาคารแห่งชาติ
   - 5.5 ธนาคารสาขา
   - 5.6 ตัวแทนธนาคารต่างประเทศ
   - 5.7 นิติบุคคลที่ดำเนินกิจการธนาคารและได้รับการอนุญาตตามมาตรา 25 แห่งพระราชบัญญัติธนาคารรัฐบาลกลาง (Federal Reserve Act)

---

[37] United State Code, (Title 18 : Crimes and Criminal Procedure, section 1005). [online] Available from : http://caselaw.lp.findlaw.com.

องค์ประกอบความผิดตามมาตรา 1006[38] มีรายละเอียดดังนี้

1. ผู้ใดซึ่งเป็นเจ้าพนักงาน ตัวแทน ลูกจ้าง หรือผู้ที่มาทำการติดต่อกับสถาบันทางการเงิน โดยเจตนาฉ้อโกงสถาบันทางการเงิน ประชาชน บริษัท หรือบุคคลทั่วไป หรือเพื่อหลอกลวงพนักงานเจ้าหน้าที่ ผู้ตรวจสอบหรือตัวแทนของสถาบันทางการเงิน หรือหน่วยงานของประเทศสหรัฐอเมริกา โดยทำการใส่ข้อมูลไม่ถูกต้องในสมุดบัญชีธนาคาร รายงาน หรือรายการทางบัญชีของสถาบันทางการเงินนั้น หรือโดยปราศจากอำนาจในการเพิกถอนคำสั่งให้ธนาคารจ่าย หรือทำการยอมรับ หรือออกข้อกำหนดทางบันทึกต่างๆ
2. ผู้ใดโดยเจตนาฉ้อโกงต่อประเทศสหรัฐอเมริกา ตัวแทน หรือบริษัท หรือนิติบุคคล ทั้งนี้รวมถึงผู้ที่ได้รับเงิน ผลประโยชน์ ทรัพย์สิน ผลกำไรผ่านการโอนทางบัญชี ไม่ว่าทางตรงหรือทางอ้อม หรือผู้ที่มีส่วนร่วมในการกระทำความผิด
3. สถาบันทางการเงินการธนาคารตามมาตรานี้ ได้แก่
   - 3.1 บริษัทประกันภัยเงินฝากของรัฐบาลกลาง
   - 3.2 กลุ่มสหกรณ์เงินกู้แห่งชาติ
   - 3.3 สำนักงานตรวจตราการออมทรัพย์แห่งชาติ
   - 3.4 บริษัทสินเชื่อหรือทรัสต์
   - 3.5 ธนาคารสินเชื่อที่อยู่อาศัย
   - 3.6 คณะกรรมการรัฐบาลกลางของธนาคารเพื่อการเคหะ
   - 3.7 ธนาคารสินเชื่อเพื่อการเกษตร
   - 3.8 องค์กรพัฒนาเคหะหรือชุมชนชานเมือง
   - 3.9 สถาบันประกันข้าวโพด
   - 3.10 เลขาธิการเพื่อการเกษตร
   - 3.11 ตัวแทนของธนาคารเพื่อการเกษตรหรือผู้มีส่วนร่วมในธนาคารดังกล่าว

---

[38] United State Code,(Title 18 : Crimes and Criminal Procedure, section 1006). [online] Available from : http://caselaw.lp.findlaw.com.

3.12 บริษัทที่ให้กู้ยืม รับฝากเงิน ประกันภัย ให้เครดิตหรือออมทรัพย์

3.13 นิติบุคคลที่อยู่ภายใต้การควบคุมของสถาบันต่างๆ ในประเทศสหรัฐอเมริกา (นอกเหนือจากที่ระบุไว้ในมาตรา 656)

3.14 สถาบันที่ได้รับการรับรองโดยบริษัทประกันเงินฝากของรัฐบาลกลาง หรือ โดยคณะกรรมการแห่งสหกรณ์เงินกู้แห่งประเทศสหรัฐอเมริกา

3.15 บริษัทลงทุนรายย่อย

องค์กระกอบความผิดตามมาตรา 1007[39] มีรายละเอียด ดังนี้

1. ผู้ใดซึ่งโดยเจตนาในการจัดทำ หรือนำมาซึ่งข้อมูลใด ๆ ที่เกี่ยวข้องกับพิจารณาถึงความน่าเชื่อถือของระบบ
2. จัดทำ นำมาซึ่งข้อมูลที่ไม่ถูกต้อง หลอกลวง หรือปลอมแปลงรายการทางบัญชี เอกสาร หรือสิ่งหนึ่งสิ่งใด
3. โดยมีวัตถุประสงค์ในการใช้อิทธิพลในทางใดๆ ต่อบริษัทประกันเงินฝากของธนาคารรัฐบาลกลาง ซึ่งบริษัทประกันเงินฝากของรัฐบาลกลางเป็นหน่วยงานที่ทำหน้าที่ดูแลระบบบัญชีเงินฝากของธนาคารรัฐบาลกลางทั้งหมด

<u>บทกำหนดโทษ</u>

1. ผู้ใดกระทำความผิดตามที่ได้กำหนดไว้ในมาตรา 1005 , 1006 หรือมาตรา 1007 ผู้นั้นมีโทษปรับไม่เกิน 1,000,000 ดอลลาร์สหรัฐ หรือ มีโทษจำคุกไม่เกิน สามสิบ ปี หรือทั้งจำทั้งปรับ
2. ความผิดดังกล่าวอยู่ภายใต้การบังคับใช้ของมาตรการริบทรัพย์สินตามมาตรา 981 และมาตรา 982 แห่งประมวลกฎหมายฉบับนี้ ซึ่งจะได้อธิบายในรายละเอียดต่อไป

---

[39] United State Code, (Title 18 : Crimes and Criminal Procedure, section 1007). [online] Available from : http://caselaw.lp.findlaw.com.

2. ความผิดต่อการฉ้อโกงธนาคาร

ความผิดต่อการฉ้อโกงธนาคาร ตามบทบัญญัติแห่งประมวลกฎหมายอาญา มาตรา 1344 ซึ่งกำหนดถึงการกระทำอันเป็นการ วางแผน หรือใช้เล่ห์อุบายต่าง ๆ ในการฉ้อโกงสถาบันทางการเงิน เพื่อให้ได้มาซึ่งเงิน เงินฝาก เครดิต ทรัพย์สิน หรือมาตรการความปลอดภัย ซึ่งมาตรานี้เป็นการกำหนดลักษณะของความผิดอย่างกว้างไว้ถึง การกระทำการพยายามกระทำการ วางแผนหรือใช้อุบายอย่างหนึ่ง เพื่อการฉ้อโกง หลอกลวง ฉ้อฉลเพื่อให้ได้มาซึ่งเงิน เครดิต มาตรการความปลอดภัยของธนาคารหรือสถาบันทางการเงิน ซึ่ง "มาตรการความปลอดภัย" นั้น หมายความรวมถึง "เครื่องมือในการชำระหนี้" ตามความหมายของคำจำกัดความคำว่า "เครื่องมือการชำระหนี้" แห่งมาตรา 916 ของกฎของสถาบันทางการเงินและการควบคุมอัตราดอกเบี้ย[40]

หากพิจารณาความหมาย คำว่า "เครื่องมือในการชำระหนี้" ตามกฎของสถาบันทางการเงินและการควบคุมอัตราดอกเบี้ย มาตรา916 ได้กำหนดคำจำกัดความไว้ หมายถึง บัตร รหัส หรือสื่อใดๆ ที่บุคคลหรือผู้ใช้บริการทางการเงินนำมาใช้ในการโอนเงินทางอิเล็กทรอนิกส์ ดังนั้น ความผิดตามมาตรานี้ซึ่งกำหนดลักษณะความผิดการฉ้อโกง หลอกลวง ฉ้อฉลเพื่อให้ได้มาซึ่งเงิน เครดิตของธนาคารหรือสถาบันทางการเงินแล้วยังรวมถึง บัตร รหัส หรือสื่อทางอิเล็กทรอนิกส์ใดๆ ในการเข้าถึงการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งองค์ประกอบความผิดตามมาตรา 1344[41] ดังกล่าวมีรายละเอียดดังนี้

1. ผู้ใดซึ่งโดยเจตนากระทำการ พยายามกระทำการวางแผน หรือใช้เล่ห์อุบายฉ้อโกงสถาบันทางการเงิน
2. โดยการกระทำการอย่างหนึ่งอย่างใด แสดง การให้สัญญาอันเป็นเท็จ การหลอกลวง หรือการฉ้อฉล
3. เพื่อให้ได้รับซึ่งเงิน เงินฝาก เครดิต ทรัพย์สิน มาตรการความปลอดภัย หรือทรัพย์สินอื่นใดที่อยู่ในความครอบครอง หรืออยู่ภายใต้การเก็บรักษา หรือควบคุมของสถาบันทางการเงิน

---

[40] United State Code, (Title 18 : Crimes and Criminal Procedure, section 1344 see section 513 (c)(3)(1)). [online] Available from : http://caselaw.lp.findlaw.com.

[41] Ibid, Section 1344.

บทกำหนดโทษ

1. ผู้นั้นมีโทษปรับไม่เกิน 1,000,000 ดอลลาร์สหรัฐ หรือ มีโทษจำคุกไม่เกิน สามสิบ ปี หรือทั้งจำทั้งปรับ
2. ความผิดดังกล่าวอยู่ภายใต้การบังคับใช้ของมาตรการริบทรัพย์สินตามมาตรา 981 และมาตรา 982 แห่งประมวลกฎหมายฉบับนี้ ซึ่งจะได้อธิบายในรายละเอียดต่อไป

3.2.1.2.3 ความผิดเกี่ยวกับบัตร รหัส หรือสื่อทางอิเล็กทรอนิกส์

ประมวลกฎหมายอาญานี้ ได้มีการกำหนดบทบัญญัติอันเป็นความผิดเกี่ยวกับบัตร รหัส หรือสื่ออิเล็กทรอนิกส์ในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ไว้ในหลายลักษณะความผิด ดังนี้

1. ความผิดต่อการปลอมแปลงบัตร รหัส หรือสื่อทางอิเล็กทรอนิกส์

ความผิดต่อการปลอมแปลงและการปลอมบัตร รหัส หรือสื่ออิเล็กทรอนิกส์ในการโอนเงินทางอิเล็กทรอนิกส์ได้กำหนดไว้ในเป็นความผิดหนึ่งตามมาตรา 513 ว่าด้วยมาตรการความปลอดภัยของรัฐ และธุรกิจภาคเอกชน โดยมาตราดังกล่าวได้กำหนดให้บัตรที่มีแถบแม่เหล็ก (เงินพลาสติก) รหัส หรือสื่อทางอิเล็กทรอนิกส์ในการโอนเงินทางอิเล็กทรอนิกส์เป็นส่วนหนึ่งของมาตรการความปลอดภัยของรัฐ โดยถือเป็นเครื่องมือในการชำระหนี้ ตามมาตรา 916 แห่งกฎของสถาบันทางการเงินและการควบคุมอัตราดอกเบี้ย

ด้วยเหตุว่า "มาตรการความปลอดภัย" ตามมาตรา 513 (c) นี้ได้กำหนดให้รวมถึง "เครื่องมือในการชำระหนี้" ตามมาตรา 916 ของกฎของสถาบันทางการเงินและการควบคุมอัตราดอกเบี้ย[42] และตามความหมายของคำว่า "เครื่องมือการชำระหนี้" แห่งกฎของสถาบันทางการเงินและการควบคุมอัตราดอกเบี้ยตามมาตรา 916 ได้กำหนดคำจำกัดความคำว่า "เครื่องมือในการชำระหนี้" ไว้หมายถึง บัตร รหัสหรือสื่อใดๆ ที่บุคคลหรือผู้ใช้บริการทางการเงินนำมาใช้ในการโอนเงินทางอิเล็กทรอนิกส์ ดังนั้นการปลอมและการปลอมแปลงมาตรการความปลอดภัย

---

[42] United State Code, (Title 18 : Crimes and Criminal Procedure, section 513 (c)(3)(1)). [online] Available from : http://caselaw.lp.findlaw.com.

แห่งรัฐ และธุรกิจภาคเอกชนจึงบังคับใช้รวมถึงการปลอมแปลง การปลอมบัตรที่มีแถบแม่เหล็ก รหัส หรือสื่อใดๆ ทางอิเล็กทรอนิกส์ในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ด้วย

ซึ่งความผิดตาม มาตรา 513 [43] ดังกล่าว มีองค์ประกอบความผิดดังนี้

1. ผู้ใดกระทำการ เปลี่ยนแปลง ปลอมแปลงมาตรการความปลอดภัยแห่งรัฐ องค์กรทางการเมือง หรือหน่วยงานต่าง ๆ หรือกระทำการปลอมมาตรการความปลอดภัยของรัฐ องค์กรทางการเมือง หน่วยงานต่างๆ แห่งรัฐหรือรัฐบาล โดยเจตนาหลอกลวงบุคคล องค์กร หรือหน่วยงานแห่งรัฐหรือรัฐบาลดังกล่าว
2. ผู้ใดกระทำการ การได้รับ การดำเนินการ การขายหรือการโอน โดยวิธีหนึ่งวิธีใด โดยการปลอม หรือการปลอมแปลงมาตรการความปลอดภัย และเจตนาให้ได้รับประโยชน์จากกรณีดังกล่าว
3. มาตรการความปลอดภัย ตามมาตรา 513 (c) นี้หมายถึง
   - 3.1 เอกสาร, ใบรับรองหุ้น, หุ้นกู้, ใบหุ้น, พันธบัตรรัฐบาล, สมุดรับรองเงินฝาก, ดอกเบี้ย, เช็ค, ดร๊าฟท์, ใบรับรอง, เครื่องมือในการชำระหนี้ซึ่งเป็นไปตามคำจำกัดความแห่งมาตรา 916 (c) แห่งกฎหมายฉบับนี้, คำสั่งทางการเงิน, เช็คเดินทาง, หนังสือรับรองการจ่ายเงินของธนาคาร, ใบเก็บรักษาสินค้าในคลังสินค้า, ใบบันทึกรายการในการทำรายการทางบัญชี, พยานหลักฐานที่ปราศจากข้อสงสัย, บันทึกที่รับรองเรื่องด้านดอกเบี้ย, ใบรับรองทางการเงินต่างๆ
   - 3.2 เครื่องมือในการแสดงพยานหลักฐานแก่สินค้า, การค้าและการพาณิชย์
   - 3.3 เครื่องมือในการแสดงถึง ความสำคัญของมาตรการด้านความปลอดภัย
   - 3.4 หนังสือรับรองต่างๆ
   - 3.5 แบบฟอร์มต่างๆ ของธนาคาร

---

[43] United State Code,(Title 18 : Crimes and Criminal Procedure, section 513). [online] Available from : http://caselaw.lp.findlaw.com.

<u>บทกำหนดโทษ</u>

ผู้นั้นมีโทษปรับไม่เกิน 250,000 ดอลลาร์สหรัฐ หรือจำคุกไม่เกิน สิบ ปี หรือทั้งจำทั้งปรับ

2. ความผิดต่อการแสดงอุปกรณ์อิเล็กทรอนิกส์ปลอม หรือข้อมูลเท็จ เพื่อทำการฉ้อโกงการโอนเงินทางอิเล็กทรอนิกส์

มาตรา 514 (a)(3)[44] ได้กำหนดถึงความผิดต่อโดยการแสดง หรือหลอกลวงมาตรการความปลอดภัย เพื่อทำการโอนผ่านอุปกรณ์อิเล็กทรอนิกส์ เอกสาร หรือมาตรการความปลอดภัยตามมาตรา 513 (c) ของระบบการเงินการธนาคาร ซึ่งจะเห็นได้ว่าความผิดดังกล่าวเป็นส่วนหนึ่งภายใต้กระบวนการโอนเงินทางอิเล็กทรอนิกส์ ดังนั้นจึงถือเป็นส่วนหนึ่งของอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ โดยมีองค์ประกอบความผิดดังนี้

1. ผู้ใดเจตนาฉ้อโกงต่อระบบอำนวยความสะดวกทางการพาณิชย์ระหว่างรัฐหรือการพาณิชย์ระหว่างประเทศ รวมถึงการใช้การส่งข้อมูลผ่านไปรษณีย์ โทรเลข วิทยุ หรืออุปกรณ์สื่อสารอิเล็กทรอนิกส์
2. ทำการแสดงอุปกรณ์อิเล็กทรอนิกส์ เอกสาร หรือสิ่งใดสิ่งหนึ่งอื่นๆ อันเป็นเท็จหรือปลอม
3. ทำการแสดง การให้ความหมาย หรือวางเล่ห์กลต่อการจัดการหรือการวางอุบายต่อมาตรการความปลอดภัยตามมาตรา 513 (c) ซึ่งหมายถึงบัตร รหัส หรือสื่ออุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการโอนเงินทางอิเล็กทรอนิกส์ หรืออุปกรณ์อิเล็กทรอนิกส์ทางการธนาคารอื่นๆ ซึ่งอยู่ภายใต้การควบคุมดูแลของหน่วยงานที่มีอำนาจหน้าที่ของประเทศสหรัฐอเมริกาหรือหน่วยงานต่างๆ

---

[44] United State Code,(Title 18 : Crimes and Criminal Procedure, section 514(a)(3)). [online] Available from : http://caselaw.lp.findlaw.com.

4. เพื่อทำการส่งผ่าน การขนส่ง การลำเลียง การเคลื่อนย้าย การโอน หรือพยายามกระทำเช่นนั้นเพื่อไปยังอีกที่หนึ่ง หรือจากอีกที่หนึ่ง หรือทั่วประเทศสหรัฐอเมริกา

บทกำหนดโทษ

ผู้นั้นมีโทษปรับไม่เกิน 250,000 ดอลลาร์สหรัฐ หรือมีโทษจำคุกไม่เกิน สิบ ปี หรือทั้งจำทั้งปรับ

3.2.1.2.4 ความผิดต่อการเข้าถึงบัตร รหัส หรือสื่ออิเล็กทรอนิกส์

ประมวลกฎหมายอาญานี้ได้กำหนดบทบัญญัติที่เกี่ยวข้องกับ ความผิดต่อการฉ้อโกงการเข้าถึงสื่อหรืออุปกรณ์อิเล็กทรอนิกส์ หรือความผิดอันเป็นการฉ้อโกงบัตรเครดิต ซึ่งได้บัญญัติไว้ในประมวลกฎหมายอาญา บรรพที่ 18 มาตรา 1029 (18 U.S.C.1029) โดยได้กำหนดการกระทำอันเป็นความผิดต่อการเข้าถึงเครื่องหรืออุปกรณ์ทางอิเล็กทรอนิกส์ไว้ในฐานความผิด "การเข้าถึง" หรืออาจเรียกบทบัญญัติดังกล่าวไว้โดยทั่วไปว่า "พระราชบัญญัติควบคุมการฉ้อโกงบัตรเครดิต (Credit Card Abuse Act)" และความผิดลักษณะดังกล่าวเป็นความผิดที่เกิดขึ้นในส่วนหนึ่งของกระบวนการโอนเงินทางอิเล็กทรอนิกส์

โดยความผิดเกี่ยวกับการฉ้อโกงการเข้าถึงสื่อ หรือเครื่องอิเล็กทรอนิกส์ มาตรา 1029 นั้น ได้กำหนดฐานความผิดไว้หลายฐานลักษณะความผิด กล่าวคือ

"การเข้าถึงเครื่องอิเล็กทรอนิกส์" หมายถึง การเข้าถึงบัญชีโดยวิธีหนึ่งวิธีใด โดยการสามารถใช้ เข้าถึงเครื่องอิเล็กทรอนิกส์ อุปกรณ์อิเล็กทรอนิกส์ดังกล่าว หรือเชื่อมโยงการเข้าถึงเครื่องอิเล็กทรอนิกส์กับอุปกรณ์อิเล็กทรอนิกส์อีกอุปกรณ์อิเล็กทรอนิกส์หนึ่ง รวมถึงบัตรที่มีแถบแม่เหล็ก, บัตรที่ใช้แถบโลหะ, รหัส หรือหมายเลขเฉพาะทางบัญชี หมายเลขประจำเครื่องอิเล็กทรอนิกส์ หมายเลขเฉพาะของเครื่องโทรศัพท์เคลื่อนที่ หรือหมายเลขประจำตัวประชาชน รวมถึงการให้บริการสื่อสารโทรคมนาคมอย่างหนึ่งอย่างใด อุปกรณ์ทางอิเล็กทรอนิกส์ หรือเครื่องมือเฉพาะอื่นๆ เพื่อให้ได้รับซึ่งเงิน สินค้า บริการ หรือสิ่งหนึ่งสิ่งใดอันมีมูลค่า หรือสิ่งหนึ่งสิ่งใดนั้นสามารถใช้ในการโอนเงินรวมถึงการโอนเงินทางอิเล็กทรอนิกส์

"การหลอกลวงซึ่งการเข้าถึงเครื่องอิเล็กทรอนิกส์" หมายถึง การเข้าถึงเครื่องอิเล็กทรอนิกส์โดยการกระทำอันเป็นการหลอกลวง ปลอม เปลี่ยนแปลง ปลอมลายมือ หรือการเพิ่มเติม หรือหลอกลวงลักษณะเฉพาะของการเข้าถึงข้อมูลทางอิเล็กทรอนิกส์

"การเข้าถึงเครื่องอิเล็กทรอนิกส์โดยปราศจากอำนาจ" หมายถึง การเข้าถึงเครื่องอิเล็กทรอนิกส์ ซึ่งเป็นการกระทำอันเป็นการทำให้สูญหาย ขโมย การยุติ การเพิกถอน การยกเลิก หรือการได้รับมาซึ่งสิ่งหนึ่งสิ่งใดโดยการหลอกลวง

ทั้งนี้ มาตรา 1029[45] ได้กำหนดลักษณะของความผิดที่อาศัยฐานความผิดที่กล่าวข้างต้นเป็นองค์ประกอบสำคัญในการกระทำความผิด และถือเป็นความผิดสำคัญตามมาตรานี้ โดยมีหลายลักษณะความผิด กล่าวคือ

ลักษณะที่ 1 ผู้ใดซึ่ง สร้าง ใช้ หรือการสื่อสาร หรือการส่งผ่านอย่างหนึ่งอย่างใดหรือมากกว่านั้นในการหลอกลวงการเข้าถึงเครื่องอิเล็กทรอนิกส์ โดยเจตนาฉ้อโกง ตามมาตรา 1029 (a) (1)

ลักษณะที่ 2 ผู้ใดซึ่ง สื่อสาร หรือการใช้ประโยชน์อย่างหนึ่งอย่างใดหรือมากกว่านั้นโดยเจตนาฉ้อโกง เพื่อการเข้าถึงเครื่องอิเล็กทรอนิกส์โดยปราศจากอำนาจภายในระยะเวลาหนึ่ง ปี และการกระทำเช่นนั้นภายในระยะเวลาดังกล่าวทำให้ได้รับประโยชน์อย่างหนึ่งอย่างใดที่มีมูลค่ารวมถึง 1,000 ดอลลาร์สหรัฐ หรือมากกว่านั้น ตามมาตรา 1029 (a) (2)

ลักษณะที่ 3 ผู้ใดซึ่ง ครอบงำอุปกรณ์อิเล็กทรอนิกส์ สิบห้าครั้ง หรือมากกว่านั้น โดยเจตนาฉ้อโกงเพื่อการหลอกลวงการเข้าถึงเครื่องอิเล็กทรอนิกส์โดยปราศจากอำนาจ ตามมาตรา 1029 (a) (3)

ลักษณะที่ 4 ผู้ใดซึ่ง สร้าง การส่งผ่านอย่างหนึ่งอย่างใดเพื่อการควบคุม เก็บรักษา ครอบงำอุปกรณ์อิเล็กทรอนิกส์ หรือการเข้าถึงเครื่องอิเล็กทรอนิกส์ดังกล่าวโดยเจตนาฉ้อโกง ตามมาตรา 1029 (a) (4)

---

[45] United State Code,(Title 18 : Crimes and Criminal Procedure, section 1029). [online] Available from : http://caselaw.lp.findlaw.com.

ลักษณะที่ 5 ผู้ใดซึ่ง กระทำการอันมีผลกระทบต่อการเปลี่ยนแปลงทางบัญชีในการเข้าถึงเครื่องอิเล็กทรอนิกส์หนึ่งครั้ง หรือมากกว่านั้น โดยเจตนาฉ้อโกงในเพื่อออกคำสั่งถึงบุคคลอีกคนหนึ่งหรือบุคคลหนึ่งบุคคลใดในการได้รับการชำระเงิน หรือสิ่งหนึ่งสิ่งใดภายในระยะเวลา หนึ่ง ปี ที่มีมูลค่ารวมเทียบเท่าตั้งแต่ 1,000 ดอลลาร์สหรัฐหรือมากกว่านั้น ตามมาตรา 1029 (a) (5)

ลักษณะที่ 6 ผู้ใดซึ่ง ออกคำสั่งเพื่อการเข้าถึงเครื่องอิเล็กทรอนิกส์โดยปราศจากอำนาจ เพื่อการฉ้อโกงที่มีวัตถุประสงค์เจตนาชักชวนบุคคลหนึ่งบุคคลใดในการส่งคำสั่งในการเข้าถึงเครื่องอิเล็กทรอนิกส์ดังกล่าวหรือ ขายข้อมูลเพื่อให้ได้มาซึ่งรหัสหรือการร้องขอใดๆ เพื่อการเข้าถึงข้อมูลทางอิเล็กทรอนิกส์ ตามมาตรา 1029 (a) (6)

ลักษณะที่ 7 ผู้ใดซึ่ง โดยเจตนาฉ้อโกงในการใช้ การสร้าง หรือการสื่อสารอย่างหนึ่งอย่างใดในกรณีดังกล่าว เพื่อการควบคุม เก็บรักษา หรือครอบงำซึ่งอุปกรณ์สื่อสารโทรคมนาคม โดยการดัดแปลงหรือเปลี่ยนแปลงหรือกระทำโดยวิธีใดๆที่ทำให้สามารถใช้บริการทางโทรคมนาคมได้โดยปราศจากอำนาจ ตามมาตรา 1029 (a) (7)

ลักษณะที่ 8 ผู้ใดซึ่ง โดยเจตนาฉ้อโกงในการใช้ การสร้าง หรือการสื่อสารอย่างหนึ่งอย่างใด เพื่อการควบคุม เก็บรักษา หรือครอบงำอุปกรณ์ในการตรวจดูการเข้าถึงเครื่องอิเล็กทรอนิกส์ดังกล่าว ตามมาตรา 1029 (a) (8) ทั้งนี้ "อุปกรณ์ในการตรวจดูการเข้าถึงเครื่องอิเล็กทรอนิกส์" หมายถึง อุปกรณ์ทางอิเล็กทรอนิกส์ หรือเครื่องมือที่สามารถใช้ในการดักฟังเครือข่าย ดักฟังการสื่อสาร โทรคมนาคม หรือหมายเลขเครื่องอิเล็กทรอนิกส์ หมายเลขโทรศัพท์เคลื่อนที่ หรือหมายเลขเฉพาะอื่นๆ อันเป็นรหัสสำคัญในการสื่อสารหรือการส่งผ่านโอนเงินทางอิเล็กทรอนิกส์ ตามมาตรา 1029 (c) (8)

ลักษณะที่ 9 ผู้ใดซึ่งใช้ สร้าง หรือสื่อสารอย่างหนึ่งอย่างใดในการควบคุม หรือเก็บรักษา หรือครอบงำซึ่งเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ โดยรู้ถึงโครงสร้างในการเข้าถึง หรือการดัดแปลงข้อมูลเฉพาะของการสื่อสารโทรคมนาคมเพื่อใช้ในกรณีดังกล่าว หรือให้ได้รับซึ่งอุปกรณ์โทรคมนาคม หรือการใช้ซึ่งอุปกรณ์โทรคมนาคม หรือได้รับบริการทางโทรคมนาคมโดยปราศจากอำนาจ

ทั้งนี้การกระทำละเมิดต่ออุปกรณ์ที่ได้ประกอบขึ้นหรือการติดต่อสื่อสารข้างต้น และผู้กระทำความผิดอาจอ้างว่าเป็นกรณีป้องกันโดยชอบด้วยกฎหมายได้ กรณีการกระทำ

ที่เกิดขึ้นนั้นอยู่ในส่วนที่เกี่ยวข้องสำหรับการวิจัย และพัฒนาเครือข่ายการติดต่อสื่อสารที่มีวัตถุประสงค์โดยชอบด้วยกฎหมาย

ลักษณะที่ 10 ผู้ใดซึ่งโดยเจตนาฉ้อโกงในการออกบัตรหรือการจัดการอย่างหนึ่งอย่างใด โดยปราศจากซึ่งอำนาจของสมาชิกระบบบัตรเครดิตหรือตัวแทนของระบบดังกล่าว เพื่อการแสดงถึงการเป็นสมาชิก หรือตัวแทนแก่บุคคลอื่น หรือเพื่อการชำระเงินในหนึ่งครั้งหรือมากกว่านั้น

บทกำหนดโทษ

1. ผู้ใดการกระทำความผิดตามได้อธิบายแล้วข้างต้น ผู้นั้นมีโทษดังนี้
   1.1 หากเป็นการกระทำความผิดที่บัญญัติไว้ในข้อ 1, 2, 3, 6, 7 หรือ 10 ข้างต้น ผู้นั้นมีโทษปรับเป็นไปตามที่กำหนดไว้ในบทบัญญัติฉบับนี้ หรือมีโทษจำคุกไม่เกิน สิบ ปี หรือทั้งจำทั้งปรับ
   1.2 หากเป็นการกระทำความผิดที่บัญญัติไว้ในข้อ 4, 5, 8 หรือ 9 ข้างต้น ผู้นั้นมีโทษปรับเป็นไปตามที่กำหนดไว้ในบทบัญญัติฉบับนี้ หรือมีโทษจำคุกไม่เกิน สิบห้า ปี หรือทั้งจำทั้งปรับ
   1.3 กรณีการกระทำความผิดตามมาตรานี้และได้เกิดขึ้นภายหลังการกระทำความผิดในอีกลักษณะหนึ่งภายใต้บทบัญญัติในมาตรานี้ ผู้นั้นมีโทษปรับเป็นไปตามที่กำหนดไว้ในบทบัญญัติฉบับนี้ หรือมีโทษจำคุกไม่เกิน ยี่สิบ ปี หรือทั้งจำทั้งปรับ
2. ผู้ใดพยายามกระทำความผิด ตามที่ได้กำหนดไว้ในข้างต้นแห่งบทบัญญัติฉบับนี้ ต้องมีโทษเป็นไปตามที่กฎหมายฉบับนี้ได้กำหนดโทษสำหรับการพยายามกระทำความผิดไว้
3. ผู้ใดได้ร่วมกระทำความผิด หรือสมรู้ร่วมคิดในการกระทำความผิดซึ่งได้กำหนดไว้ข้างต้นตั้งแต่ 2 คน ขึ้นไป หรือเป็นผู้ที่มีส่วนพัวพันกับการกระทำความผิดดังกล่าว ผู้นั้นมีโทษปรับไม่เกินกว่าอัตราโทษปรับสูงสุด ซึ่งกำหนดไว้ในข้อ 3. ที่จะกล่าวต่อไป หรือมีโทษ

จำคุกไม่เกินกว่าครึ่งหนึ่งของอัตราโทษจำคุกสูงสุดที่กำหนดโทษแห่งการกระทำความผิดลักษณะนี้ไว้ หรือทั้งจำทั้งปรับ

3.2.1.2.5 ความผิดต่อการเข้าถึงเครื่องคอมพิวเตอร์โดยปราศจากอำนาจ

ความผิดต่อการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจได้บัญญัติไว้ใน Computer Fraud and Abuse Act หรือที่เรียกกันโดยทั่วไปว่า "กฎหมายควบคุมการฉ้อโกงเครื่องคอมพิวเตอร์" ซึ่งได้บัญญัติไว้ในประมวลกฎหมายอาญา บรรพที่ 18 มาตรา 1030 โดยมาตราดังกล่าวได้กำหนดการกระทำความผิดอันเป็นการเข้าถึงเครื่องคอมพิวเตอร์หรืออุปกรณ์ทางคอมพิวเตอร์โดยปราศจากอำนาจเพื่อให้ได้มาซึ่งข้อมูลหรือประโยชน์อย่างหนึ่งอย่างใด หรือทำลายหรือสร้างความเสียหายแก่คอมพิวเตอร์ หรือความผิด "การเข้าถึงโดยปราศจากอำนาจ" ต่อคอมพิวเตอร์และระบบความปลอดภัยของคอมพิวเตอร์ที่เกี่ยวข้องกับระบบการเงินการธนาคาร หรือการโอนเงินทางอิเล็กทรอนิกส์

ซึ่งตามมาตรา 1030 นี้ ได้กำหนดฐานความผิดอันเป็น "การเข้าถึงเครื่องคอมพิวเตอร์โดยปราศจากอำนาจ" หรือ "การเข้าถึงคอมพิวเตอร์หรือระบบความปลอดภัยของคอมพิวเตอร์" จึงต้องพิจารณาคำนิยามของต่างๆ ที่เกี่ยวข้อง ไม่ว่าจะเป็น คำว่า"คอมพิวเตอร์" หรือ "ระบบความปลอดภัยของคอมพิวเตอร์" หรือ "ความเสียหายต่อระบบความปลอดภัยของคอมพิวเตอร์" หรือ "รายการทางธนาคาร" ซึ่งตามมาตรา 1030[46] ได้กำหนดคำนิยามที่เกี่ยวข้องกับพระราชบัญญัติฉบับนี้ กล่าวคือ

"คอมพิวเตอร์" หมายถึง เครื่องอิเล็กทรอนิกส์, อุปกรณ์อิเล็กทรอนิกส์ สิ่งที่สัมผัสได้ การเปลี่ยนแปลงทางเคมีอิเล็กทรอนิกส์ หรือสิ่งหนึ่งสิ่งใดที่มีกระบวนการในการส่งผ่านข้อมูลด้วยความเร็วสูงผ่านอุปกรณ์อิเล็กทรอนิกส์ การคำนวณ หรือการรักษาการปฏิบัติงานหรือการเก็บรักษาข้อมูล หรือการติดต่อสื่อสารอย่างสะดวกรวดเร็วโดยการเชื่อมต่อโดยตรงกับการปฏิบัติงานทางอิเล็กทรอนิกส์ แต่ไม่รวมถึงเครื่องพิมพ์ดีดไฟฟ้า เครื่องพิมพ์ดีดอัตโนมัติ เครื่องคำนวณ หรืออุปกรณ์อิเล็กทรอนิกส์ที่มีลักษณะเช่นนั้น

---

[46] United State Code, (Title 18 : Crimes and Criminal Procedure, section 1030) [online] Available from : http://caselaw.lp.findlaw.com.

"ระบบความปลอดภัยของคอมพิวเตอร์" หมายถึง คอมพิวเตอร์สำหรับการใช้ของสถาบันทางการเงิน หรือรัฐบาลของประเทศสหรัฐอเมริกาเท่านั้น หรือในกรณีของคอมพิวเตอร์ที่ไม่ได้ใช้อยู่ในสถาบันดังกล่าว แต่ได้ถูกใช้โดยหรือสำหรับสถาบันทางการเงินหรือรัฐบาลสหรัฐอเมริกา และโดยการใช้กระทำการในการตรวจสอบการกระทำอันเป็นความผิดที่มีผลกระทบต่อสถาบันทางการเงินหรือรัฐบาลสหรัฐอเมริกา หรือซึ่งใช้ในการค้าการพาณิชย์ระหว่างรัฐ หรือระหว่างประเทศ

"ความเสียหายต่อระบบความปลอดภัยของคอมพิวเตอร์" หมายถึง การทำให้เสียหายซึ่งความสมบูรณ์ หรือความมีอยู่ของข้อมูล หรือโปรแกรม หรือระบบ หรือข่าวสาร ซึ่งเป็นเหตุให้เกิดความสูญหายที่มีมูลค่ารวมอย่างน้อย 5,000 ดอลลาร์สหรัฐ ภายในระยะเวลาหนึ่ง ปี หรือมากกว่านั้น

"รายการทางการธนาคาร" หมายถึง ข้อมูลที่ได้รับจากการบันทึกของสถาบันทางการเงินเกี่ยวกับธุรกรรมทางการธนาคารต่างๆ ของผู้ใช้บริการกับสถาบันการเงินนั้น

ทั้งนี้ตามคำนิยามตาม มาตรา 1030 นี้ข้างต้นจะเห็นได้ว่า ฐานความผิดต่าง ๆ ตามมาตรานี้มีบทบัญญัติที่ครอบคลุมถึงกระบวนการต่างๆ ภายใต้การโอนเงินทางอิเล็กทรอนิกส์ของระบบการเงินการธนาคารของประเทศสหรัฐอเมริกา ซึ่งฐานความผิด "การเข้าถึงโดยปราศจากอำนาจ" ที่เกี่ยวข้องกับกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ตามมาตรา 1030 มีองค์ประกอบของฐานความผิด ดังนี้

ลักษณะที่ 1 ผู้ใดซึ่ง, โดยเจตนาเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ หรือการใช้อำนาจในการเข้าถึงคอมพิวเตอร์นั้นเพื่อการละเมิด หรือให้ได้รับมาซึ่งข้อมูลที่บันทึกไว้ในรายการทางธนาคารของสถาบันทางการเงิน หรือข้อมูลของผู้ออกบัตร หรือข้อมูลของผู้ใช้บริการทางการเงินการธนาคาร ตามมาตรา 1030 (a)(2)(A)

ลักษณะที่ 2 ผู้ใดซึ่ง, โดยเจตนาฉ้อโกงเข้าถึงระบบความปลอดภัยของคอมพิวเตอร์โดยปราศจากอำนาจ หรือใช้อำนาจในการเข้าถึงนั้นเพื่อการละเมิด ซึ่งการกระทำดังกล่าวมีวัตถุประสงค์ในการฉ้อโกงหรือให้ได้รับมาซึ่งสิ่งหนึ่งสิ่งใดอันมีมูลค่า ยกเว้นวัตถุประสงค์ในการฉ้อโกงหรือให้ได้รับมาซึ่งสิ่งหนึ่งสิ่งใดภายในระยะเวลา หนึ่งปี มีมูลค่ารวมไม่เกิน 5,000 ดอลลาร์สหรัฐ ตามมาตรา 1030 (a)(4)

ลักษณะที่ 3 ผู้ใดซึ่ง, โดยเจตนาอันเป็นเหตุให้มีการส่งผ่านระบบ ข้อมูล รหัส หรือให้ได้มาซึ่ง หรือผลแห่งการกระทำนั้นจงใจก่อให้เกิดความเสียหายแก่ระบบความปลอดภัยของคอมพิวเตอร์ โดยปราศจากอำนาจในการกระทำดังกล่าว และการกระทำดังกล่าวได้สร้างความเสียหายแก่ระบบความปลอดภัยของคอมพิวเตอร์ ทั้งนี้ หากการกระทำความผิดข้างต้นเป็นผลเนื่องมาจากการพยายามกระทำความผิดแล้ว ความผิดดังกล่าวจะถือเป็นความผิดสำเร็จก็ต่อเมื่อการกระทำดังกล่าวได้กระทำจนเสร็จสิ้นสมบูรณ์แล้ว ตามมาตรา 1030 (a)(5)(A) และ (B)

ลักษณะที่ 4 โดยเจตนาสั่งและส่งผ่านคำสั่งจากบุคคลหนึ่งบุคคลใด สำนักงาน องค์กร สถาบันทางการศึกษา สถาบันทางการเงิน หน่วยงานรัฐบาล หน่วยงานทางด้านกฎหมายอื่นๆ โดยมีวัตถุประสงค์ในการทำลาย หรือสร้างความเสียหายต่อระบบความปลอดภัยของคอมพิวเตอร์ เพื่อให้ได้มาซึ่งเงิน หรือสิ่งหนึ่งสิ่งใดอันมีมูลค่าในการโอนทางการค้าระหว่างรัฐหรือการค้าระหว่างประเทศ ตามมาตรา 1030 (a)(7)

บทกำหนดโทษ

1. การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ ตามที่ได้กำหนดไว้ในความผิดลักษณะที่ 1. ที่กล่าวแล้วข้างต้น ซึ่ง
   1.1 การกระทำดังกล่าว หรือการพยายามกระทำความผิดดังกล่าวมิได้เกิดขึ้นภายหลังการกระทำความผิดอีกลักษณะหนึ่งภายใต้มาตรานี้ ผู้นั้นต้องมีโทษปรับเป็นไปตามที่กำหนดไว้ในบทบัญญัติฉบับนี้ หรือมีโทษจำคุกไม่เกิน หนึ่ง ปี หรือทั้งจำทั้งปรับ
   1.2 การพยายามกระทำความผิด ภายใต้วัตถุประสงค์ทางการค้าการพาณิชย์หรือผลประโยชน์ทางธุรกิจ และเป็นการละเมิดต่อสถาบันแห่งรัฐของประเทศสหรัฐอเมริกา ซึ่งข้อมูลดังกล่าวมีมูลค่ามากกว่า 5,000 ดอลลาร์สหรัฐ ผู้นั้นต้องมีโทษปรับเป็นไปตามที่กำหนดไว้ในบทบัญญัติฉบับนี้ หรือมีโทษจำคุกไม่เกิน ห้า ปี หรือทั้งจำทั้งปรับ
   1.3 การกระทำความผิด หรือการพยายามกระทำความผิดเป็นการกระทำความผิดที่เกิดขึ้นภายหลังการกระทำความผิดอีกลักษณะหนึ่งภายใต้มาตรานี้ ผู้นั้นต้องมีโทษปรับเป็นไปตามที่กำหนด

ไว้ในบทบัญญัติฉบับนี้ หรือมีโทษจำคุกไม่เกิน สิบ ปี หรือทั้งจำทั้งปรับ

2. การเข้าถึงระบบความปลอดภัยของคอมพิวเตอร์ โดยปราศจากอำนาจ หรือการส่งผ่านข้อมูลต่อระบบความปลอดภัยของคอมพิวเตอร์โดยปราศจากอำนาจ หรือการสั่งหรือส่งคำสั่งผ่านระบบความปลอดภัยของคอมพิวเตอร์ เพื่อทำลายหรือสร้างความเสียหายต่อระบบความปลอดภัยดังกล่าว ตามที่ได้กำหนดไว้ในลักษณะที่ 2. ลักษณะที่ 3. และลักษณะที่ 4 ที่กล่าวแล้วข้างต้นซึ่ง

2.1 การกระทำความผิด หรือการพยายามกระทำความผิดดังกล่าวเป็นการกระทำความผิดที่มิได้เกิดขึ้น ภายหลังการกระทำความผิดอีกลักษณะหนึ่งภายใต้มาตรานี้ ผู้นั้นต้องมีโทษปรับตามที่บัญญัติไว้ภายใต้อนุมาตรานี้ หรือมีโทษจำคุกไม่เกิน ห้า ปีหรือทั้งจำทั้งปรับ

2.2 การกระทำความผิด หรือการพยายามกระทำความผิดดังกล่าวเป็นการกระทำความผิดได้เกิดขึ้นภายหลังการกระทำความผิดอีกลักษณะหนึ่งภายใต้มาตรานี้ต้องมีโทษปรับตามที่บัญญัติไว้ภายใต้อนุมาตรานี้ หรือมีโทษจำคุกไม่เกิน สิบ ปี หรือทั้งจำทั้งปรับ

3.2.1.2.6 ความผิดต่อกิจการที่ประกอบกิจการอันเป็นความผิดทางการเงิน การธนาคาร

ตามมาตรา 225 นี้ได้กำหนดมาตรการในการบังคับใช้กับธุรกิจหรือนิติบุคคลที่ประกอบกิจการอันเป็นความผิดทางการเงินการธนาคาร ทั้งนี้การโอนเงินทางอิเล็กทรอนิกส์เป็นกระบวนการหนึ่งที่อยู่ภายใต้ระบบการเงินการธนาคาร ดังนั้นการดำเนินกิจการอันเป็นความผิดทางการเงินการธนาคารที่กำหนดไว้ในมาตรา225 จึงมีองค์ประกอบความผิดบางประการที่เกี่ยวข้องกับความผิดที่เกิดขึ้นในการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งเป็นความผิดที่

ได้อธิบายไปแล้วข้างต้น ดังนั้น ความผิดทางการเงินการธนาคารที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ ตามมาตรา 225[47] นี้จึงมีสาระสำคัญ ดังนี้

1. ผู้ใดจัดตั้ง จัดการ หรือควบคุม ดูแลกิจการที่ประกอบกิจการอันเป็นความผิดทางการเงินการธนาคาร
2. กิจการที่กระทำความผิดทางการเงินการธนาคารที่เกี่ยวข้องกับกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ได้แก่
   - 2.1 กิจการที่ได้กระทำความผิดตามมาตรา 215 ในการรับ ให้ ซึ่งเงินหรือประโยชน์อย่างหนึ่งอย่างใดแก่พนักงานธนาคาร ไม่ว่าจะเป็นการใช้อิทธิพลหรือการให้ค่าตอบแทน เพื่อให้ได้มาซึ่งประโยชน์อย่างหนึ่งอย่างใดจากธนาคารหรือสถาบันทางการเงิน
   - 2.2 กิจการที่ได้กระทำความผิด ตามมาตรา 656 โดยการทุจริตต่อหน้าที่ของพนักงานเจ้าหน้าที่หรือลูกจ้างของธนาคารหรือสถาบันทางการเงิน
   - 2.3 กิจการที่ได้กระทำความผิดตามมาตรา 657 โดยการทุจริตต่อหน้าที่ของพนักงานเจ้าหน้าที่หรือลูกจ้าง เพื่อประโยชน์อย่างหนึ่งอย่างใดจากสถาบันทางการเงินนอกเหนือจากสถาบันทางการเงินที่กำหนดไว้ในมาตรา 656
   - 2.4 กิจการที่ได้กระทำความผิดต่อมาตรา 1005 โดยการกระทำอย่างหนึ่งอย่างโดอันเป็นการเปลี่ยนแปลงข้อมูลต่อบันทึกรายงาน และการเปลี่ยนแปลงทางบัญชีของธนาคาร หรือสถาบันทางการเงิน
   - 2.5 กิจการที่ได้กระทำความผิดต่อมาตรา 1006 โดยการกระทำอย่างหนึ่งอย่างใด อันเป็นการเปลี่ยนแปลงข้อมูลต่อบันทึกของสถาบันของรัฐบาลกลาง รายงาน และการเปลี่ยนแปลงทางบัญชี
   - 2.6 กิจการที่ได้กระทำความผิดต่อมาตรา 1344 โดยการฉ้อโกงธนาคาร

---

[47] United State Code, (Title 18 : Crimes and Criminal Procedure, section 225) [online] Available from : http://caselaw.lp.findlaw.com.

3. เพื่อให้ได้รับเงินตั้งแต่ 5,000,000 ดอลลาร์สหรัฐหรือมากกว่านั้น หรือเป็นธุรกิจขนาดใหญ่ที่ได้รับผลประโยชน์มหาศาลในช่วงเวลาการประกอบการภายในระยะเวลา ยี่สิบสี่เดือน

<u>บทกำหนดโทษ</u>

1. กรณีผู้กระทำความผิดเป็นบุคคลธรรมดา ผู้นั้นมีโทษปรับไม่เกิน 1,000,000 ดอลลาร์สหรัฐ หรือ มีโทษจำคุกไม่น้อยกว่า สิบ ปี หรือทั้งจำทั้งปรับ
2. กรณีผู้กระทำความผิดเป็นนิติบุคคล ผู้นั้นมีโทษปรับไม่เกิน 20,000,000 ดอลลาร์สหรัฐ หรือมีโทษจำคุกตลอดชีวิต หรือทั้งจำทั้งปรับ

3.2.1.2.7 ความผิดต่อการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์

ประมวลกฎหมายอาญานี้ ได้กำหนดความผิดต่อการฟอกเงินในลักษณะต่างๆ ไว้ในบทบัญญัติที่เรียกว่า Money Laundering Control Act หรือ "กฎหมายควบคุมการฟอกเงิน" ซึ่งบัญญัติไว้ในประมวลกฎหมายอาญา บรรพที่ 18 มาตรา 1956 โดยมาตราดังกล่าวได้กำหนดถึงความผิดต่อการฟอกเงินในลักษณะต่างๆ ไว้ และได้รวมถึงการกระทำความผิดอันเป็นการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ด้วย ซึ่งตามมาตรา 1956[48] ดังกล่าวมีสาระสำคัญดังนี้

1. ผู้ใดซึ่งโดยรู้ว่าทรัพย์สิน ซึ่งรวมอยู่ในการโอนเงินทางธนาคาร หรือการพยายามการกระทำการนั้น ซึ่งความเป็นจริงทรัพย์สินนั้น มีที่มาจากกระบวนการอันเป็นความผิดเฉพาะทางกฎหมาย โดยการกระทำดังกล่าวเป็นการกระทำซึ่ง
   1.1 โดยเจตนาสนับสนุนการกระทำการอันเป็นความผิดเฉพาะทางกฎหมายนั้น หรือ

---

[48] United State Code,(Title 18 : Crimes and Criminal Procedure, section 1956) [online] Available from : http://caselaw.lp.findlaw.com.

1.2 โดยเจตนากระทำความผิดที่มีส่วนเกี่ยวข้องกับการกระทำความผิดอันเป็นการละเมิดพระราชบัญญัติภาษี มาตรา 7201 หรือ 7206

1.3 โดยเจตนาเปลี่ยนแปลงทางบัญชีทั้งหมดหรือแต่บางส่วน เพื่อปกปิด ซ่อนเร้นประเทศ พื้นที่ท้องถิ่น แหล่งที่มา เจ้าของ เพื่อควบคุมการกระทำอันเป็นความผิดเฉพาะทางกฎหมาย หรือเพื่อหลีกเลี่ยงการรายงานการเปลี่ยนแปลงทางบัญชีนั้น ซึ่งถูกกำหนดไว้ภายใต้กฎหมายแห่งรัฐหรือกฎหมายแห่งรัฐบาลกลาง

2. ผู้ใดทำการโอน หรือการพยายามโอนผ่านอุปกรณ์อิเล็กทรอนิกส์ หรือโอนเงินดังกล่าวจากสถานที่หนึ่งภายในหรือภายนอกประเทศสหรัฐอเมริกา ไปยังอีกสถานที่หนึ่งภายในหรือภายนอกประเทศสหรัฐอเมริกา โดยการกระทำดังกล่าวเป็นการกระทำซึ่ง

2.1 โดยเจตนาสนับสนุนการกระทำการอันเป็นความผิดเฉพาะทางกฎหมาย

2.2 โดยเจตนาทำการขนส่ง ส่งผ่าน หรือโอน ผ่านอุปกรณ์อิเล็กทรอนิกส์หรือเงิน ซึ่งอุปกรณ์อิเล็กทรอนิกส์หรือเงินนั้นได้แสดงถึงที่มาของการขนส่ง ส่งผ่าน หรือการโอนนั้นทั้งหมดหรือแต่บางส่วน เพื่อปกปิด ซ่อนเร้นต่อประเทศชาติ พื้นที่ท้องถิ่น แหล่งที่มา เจ้าของ หรือเพื่อควบคุมกระบวนการในการกระทำอันเป็นความผิดเฉพาะทางกฎหมาย หรือเพื่อหลีกเลี่ยงการรายงานการเปลี่ยนแปลงทางบัญชีทางการเงินการธนาคารนั้น ซึ่งได้กำหนดไว้ภายใต้กฎหมายแห่งรัฐหรือกฎหมายแห่งรัฐบาลกลาง

3. ผู้ใด โดยเจตนาจงใจสนับสนุนการกระทำการอันเป็นความผิดเฉพาะทางกฎหมาย เพื่อปกปิด หรือซ่อนเร้นประเทศ พื้นที่ท้องถิ่น แหล่งที่มา เจ้าของ หรือเพื่อควบคุมทรัพย์สินอันเชื่อว่ามาจากกระบวนการอันเป็นความผิดเฉพาะทางกฎหมาย หรือเพื่อหลีกเลี่ยงการรายงานการเปลี่ยนแปลงทางบัญชีนั้น ซึ่งถูกกำหนดไว้ภายใต้กฎหมายแห่งรัฐหรือกฎหมายแห่งรัฐบาล

กลางโดยการกระทำการ หรือพยายามกระทำการแสดงทรัพย์สินนั้นซึ่งมีที่มาจากการกระทำอันเป็นความผิดเฉพาะทางกฎหมาย หรือทรัพย์สินที่ใช้กระทำความผิดหรือทรัพย์สินที่ใช้อำนวยความสะดวกในการกระทำความผิด โดยมีวัตถุประสงค์ในการขนส่ง ส่งผ่านหรือโอนเงิน หรือโอนผ่านอุปกรณ์อิเล็กทรอนิกส์นั้น

จากองค์ประกอบความผิดข้างต้นจะเห็นได้ว่า ความผิดของการกระทำการโอนเงินที่มีที่มาโดยมิชอบด้วยกฎหมาย หรือการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าวได้บัญญัติลักษณะความผิดไว้ 3 กรณีคือ

1. โดยรู้ว่าทรัพย์สินที่เกี่ยวข้องกับเงินที่โอนนั้นมีที่มาโดยมิชอบด้วยกฎหมาย โดยไม่จำเป็นว่าเงินหรือทรัพย์สินนั้นได้มาจากความผิดรูปแบบใดของการกระทำอันเป็นความผิดหนักตามกฎหมายสหรัฐอเมริกา และมุ่งบังคับใช้ไปถึงผู้ที่รู้เห็นเกี่ยวกับการโอนเงินเพื่อการฟอกเงินดังกล่าวด้วย

2. กระทำหรือพยายามกระทำการโอนดังกล่าว ซึ่งการกระทำดังกล่าวรวมไปถึงการริเริ่ม รวบรวม หรือมีส่วนร่วมในการริเริ่ม การรวบรวมในการโอนเงินดังกล่าวก็ถือเป็นการกระทำตามกฎหมายนี้ ("Conduct" includes initiating, concluding, or participating in initiating, or concluding a transaction)

3. ผู้สนับสนุนการกระทำความผิดข้างต้น

ซึ่งทั้งสามฐานความผิดของการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ที่กล่าวข้างต้นนั้นสามารถบังคับใช้กับ ผู้รู้เห็น ผู้กระทำ ผู้สนับสนุน ในการโอนทรัพย์สิน ที่รวมอยู่ในการโอนเงินทางอิเล็กทรอนิกส์เพื่อสนับสนุนการกระทำอันเป็นความผิดอันเป็นความผิดหนักตามประมวลกฎหมายอาญาดังกล่าว

<u>บทกำหนดโทษ</u>

1. ผู้ใดกระทำความผิดตามข้อ 1. ข้างต้น ผู้นั้นมีโทษปรับไม่เกิน 500,000 ดอลลาร์สหรัฐ หรือสองเท่าของมูลค่าแห่งทรัพย์สินที่ทำการเปลี่ยนแปลง

ทางบัญชีนั้น และถืออัตราที่มากกว่าเพียงอย่างใดอย่างหนึ่ง หรือมีโทษจำคุกไม่เกิน ยี่สิบปี หรือหรือทั้งจำทั้งปรับ

2. ผู้นั้นมีโทษปรับ ไม่เกิน 500,000 ดอลลาร์ หรือสองเท่าของมูลค่าของเงินอิเล็กทรอนิกส์ หรือเงินฝากที่ทำการขนส่ง ส่งผ่านหรือโอนนั้น และให้ถืออัตราที่มากกว่าเพียงอย่างใดอย่างหนึ่ง หรือมีโทษจำคุกไม่เกิน ยี่สิบ ปี หรืออย่างใดอย่างหนึ่ง
3. ผู้นั้นมีโทษปรับเป็นไปตามที่กำหนดไว้ในบทบัญญัติฉบับนี้ หรือ มีโทษจำคุก ไม่เกิน ยี่สิบ ปี หรือทั้งจำทั้งปรับ ในกรณีการกระทำดังกล่าวเป็นการแสดงต่อเจ้าพนักงานที่บังคับใช้กฎหมาย หรือบุคคลหนึ่งบุคคลใดที่มีอำนาจหน้าที่ดังกล่าว
4. ความผิดดังกล่าวอยู่ภายใต้การบังคับใช้ของมาตรการริบทรัพย์สินตามมาตรา 981 และมาตรา 982 แห่งประมวลกฎหมายฉบับนี้ ซึ่งจะได้อธิบายในรายละเอียดต่อไป

3.2.1.2.8 ความผิดต่อการสั่งให้โอนเงินทางอิเล็กทรอนิกส์เพื่อการฟอกเงิน

ความผิดต่อสั่งให้โอนทางการเงินหรือทรัพย์สินที่ได้มาจากกระทำความผิดตามบทบัญญัติในประมวลกฎหมายอาญา มาตรา 1957 ซึ่งหากพิจารณาถึงการกระทำความผิดอันเป็นการสั่งให้โอนทางการเงินดังกล่าวจะเห็นว่าเป็นการกระทำความผิดที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์หรืออาศัยการโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิดหรือเป็นเครื่องมือต่อการฟอกเงิน ซึ่งมาตรา 1957 [49] ได้กำหนดลักษณะการกระทำความผิดและกำหนดโทษไว้ มีสาระสำคัญดังนี้

1. การสั่งให้การโอนทางเงินในทรัพย์สินที่ได้มาจากการกระทำความผิดอันเป็นความผิดเฉพาะทางกฎหมาย โดยเจตนาสั่งให้ หรือการพยายามสั่งให้มีการโอนทางการเงิน หรือทรัพย์สิน ซึ่งมีที่มาหรือได้รับมาจากการประกอบอาชญากรรมอันเป็นความผิดเฉพาะทางกฎหมาย ที่มีมูลค่ามากกว่า 10,000 ดอลลาร์สหรัฐ ซึ่ง

---

[49] United State Code,(Title 18 : Crimes and Criminal Procedure, section 1957). [online] Available from : http://caselaw.lp.findlaw.com.

1.1 โดยการกระทำความผิดภายใต้มาตรานี้ได้เกิดขึ้นในราชอาณาจักรของประเทศสหรัฐอเมริกา หรือเขตอำนาจเฉพาะ หรือเขตอำนาจแห่งรัฐของประเทศสหรัฐอเมริกา

1.2 การกระทำความผิดภายใต้มาตรานี้ได้เกิดขึ้นนอกราชอาณาจักรของประเทศสหรัฐอเมริกา หรือเขตอำนาจพิเศษเหล่านั้น แต่ผู้กระทำการดังกล่าวเป็นบุคคลในสัญชาติแห่งประเทศสหรัฐอเมริกา

2. โดย "การโอนทางการเงิน" หมายถึง การฝาก การถอน การโอน การแลกเปลี่ยน ซึ่งมีผลกระทบต่อการค้าการพาณิชย์ระหว่างรัฐ หรือการค้าระหว่างประเทศ หรือซึ่งเงินฝากหรือเงินอิเล็กทรอนิกส์ ที่มีต่อสถาบันทางการเงิน รวมถึงการเปลี่ยนแปลงทางบัญชีที่เป็นการโอนทางการธนาคาร ภายใต้บทบัญญัติแห่งมาตรา 1956 ที่ได้อธิบายแล้วข้างต้น หรือ "ทรัพย์สินที่ได้รับมาจากการประกอบอาชญากรรม" ซึ่งหมายถึง ทรัพย์สินที่ประกอบขึ้นหรือได้รับมาจากการกระทำความผิดทางอาญา

<u>บทกำหนดโทษ</u>

1. การกระทำความผิดภายใต้มาตรานี้ให้มีโทษปรับเป็นไปตามที่ได้กำหนดไว้ในบทบัญญัติฉบับนี้ หรือ มีโทษจำคุกไม่เกินกว่า สิบ ปี หรือทั้งจำทั้งปรับ
2. กรณีข้างต้น ศาลอาจกำหนดเปลี่ยนแปลงโทษปรับได้ตามสมควร ซึ่งไม่เกิน สองเท่า ของจำนวนมูลค่าแห่งการกระทำความผิดทางอาญาที่ได้รับมาซึ่งทรัพย์สินในการโอนทางการเงินดังกล่าว
3. ความผิดดังกล่าวอยู่ภายใต้การบังคับใช้ของมาตรการริบทรัพย์สินตามมาตรา 981 และมาตรา 982 แห่งประมวลกฎหมายฉบับนี้ ซึ่งจะได้อธิบายในรายละเอียดต่อไป

3.2.1.2.9 ความผิดต่อการประกอบกิจการโอนเงินผิดกฎหมาย

หากพิจารณาถึงความผิดที่อาศัยกระบวนการโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือในการฟอกเงิน นอกเหนือความผิดต่อการโอนเงินทางอิเล็กทรอนิกส์ หรือการสั่งโอนทางอิเล็กทรอนิกส์เพื่อการฟอกเงิน ตามมาตรา 1956 หรือมาตรา 1957 แห่งกฎหมายฉบับนี้แล้ว ประมวลกฎหมายฉบับนี้ยังได้กำหนดบทบัญญัติที่บังคับใช้กับอาชญากรรมที่มีลักษณะความผิดเป็นการประกอบธุรกิจโอนเงินผิดกฎหมาย ซึ่งได้บัญญัติไว้ในมาตรา 1960[50] โดยกำหนดถึงความผิดต่อธุรกิจในการประกอบการโอนเงินที่ผิดกฎหมาย กล่าวคือ

1. ผู้ใดกระทำการ, ควบคุม, จัดการ, กำกับดูแล, กรรมการ หรือเป็นเจ้าของธุรกิจทั้งหมดหรือแต่บางส่วน
2. โดยเจตนาประกอบธุรกิจโอนเงินที่ผิดกฎหมายซึ่ง "ประกอบธุรกิจโอนเงินที่ผิดกฎหมาย" หมายถึง ธุรกิจที่ประกอบกิจการโอนเงินที่มีผลในการค้าการพาณิชย์ระหว่างรัฐหรือการค้าระหว่างประเทศ โดย
   2.1 จงใจประกอบกิจการที่ปราศจากซึ่งอำนาจในการโอนเงินแห่งรัฐ ซึ่งการประกอบการนั้นมีบทลงโทษเช่นเดียวกับผู้กระทำความผิดฐานโทษ หรือผู้กระทำความผิดร้ายแรงที่กำหนดไว้ในกฎหมายแห่งรัฐนี้ แล้วแต่กรณี,
   2.2 การยินยอมให้ล้มเหลวซึ่งการโอนเงินของธุรกิจ คำว่า "การโอนเงิน" หมายถึง การโอนที่ไม่จำกัดเฉพาะการโอนเงินของประชาชนโดยทางใดทางหนึ่ง แต่ให้หมายถึงการโอนเงินในทุก ๆ กรณี รวมถึงไม่จำกัดเฉพาะการโอนเงินภายในประเทศ ระหว่างพื้นที่ หรือโดยผ่านระบบสื่อสาร เช็ค ดร๊าฟท์ หรือการกระทำโดยวิธีหนึ่งวิธีใดเพื่อความสะดวกในการโอนเงินนั้น

---

[50] United State Code, (Title 18 : Crimes and Criminal Procedure, section 1960). [online] Available from : http://caselaw.lp.findlaw.com.

<u>บทกำหนดโทษ</u>

กรณีนี้ ผู้นั้นมีโทษปรับเป็นไปตามที่กำหนดไว้ในบทบัญญัติฉบับนี้ หรือมีโทษจำคุกไม่เกิน ห้า ปี หรือทั้งจำทั้งปรับ

3.2.2 ประเทศสหราชอาณาจักร (United Kingdom)

ประเทศสหราชอาณาจักรไม่มีการบัญญัติกฎหมาย เพื่อใช้บังคับกับการโอนเงินทางอิเล็กทรอนิกส์ไว้โดยเฉพาะ ดังนั้นโดยทั่วไปการชำระเงินทางอิเล็กทรอนิกส์แต่ละประเภทของประเทศสหราชอาณาจักรจึงอยู่ภายใต้สัญญา ระเบียบ หรือกฎหมายที่มีการยอมรับร่วมกันและอยู่ภายใต้การกำกับดูแลของธนาคารกลางแห่งสหราชอาณาจักร ตามพระราชบัญญัติธนาคารกลางแห่งสหราชอาณาจักร (The Bank of England Act, 1988) ประกอบกับหากพิจารณาถึงมาตรการทางกฎหมายประเทศสหราชอาณาจักรในการกำหนดลักษณะความผิดต่างๆ ที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์จะเห็นได้ว่า ประเทศสหราชอาณาจักรได้มีการกำหนดบทบัญญัติเพื่อบังคับใช้กับอาชญากรรมทางคอมพิวเตอร์ไว้โดยเฉพาะในพระราชบัญญัติการกระทำโดยมิชอบต่อคอมพิวเตอร์ ค.ศ. 1990 (The Computer Misuse Act,1990) ซึ่งพระราชบัญญัติฉบับนี้ได้วางบทบัญญัติเพื่อให้ใช้บังคับกับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ทั้งหมด ดังนั้น หากพิจารณาถึงอาชญากรรมที่เป็นการกระทำต่อระบบหรือกระบวนการโอนเงินทางอิเล็กทรอนิกส์ จึงอยู่ภายใต้การบังคับใช้ตามพระราชบัญญัติฉบับนี้

หากพิจารณาถึง ลักษณะของอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ นอกเหนือจากอาชญากรรมทางคอมพิวเตอร์แล้วยังมีอาชญากรรมที่อาศัยกระบวนการโอนเงินเป็นเครื่องมือในการกระทำความผิด หรือที่เรียกกันโดยทั่วไปว่า การฟอกเงิน ซึ่งประเทศสหราชอาณาจักรได้กำหนดมาตรการทางกฎหมายในการบังคับใช้กับการฟอกเงิน โดยกำหนดให้มีมาตรการในการป้องกันและปราบปรามการฟอกเงินของธนาคาร หรือสถาบันทางการเงินตามมติของสหภาพยุโรปดังที่ได้อธิบายไปแล้วข้างต้น กำหนดลักษณะความผิด และมีการวางมาตรการทางกฎหมายในการกำหนดให้มีหน่วยงานที่มีอำนาจหน้าที่เฉพาะเพื่อทำหน้าที่ในการสืบสวนสอบสวนคดีทางการเงินการธนาคาร หรือเพื่อทำการควบคุม และจัดการกับการฟอกเงินดังกล่าวโดยเฉพาะ

ด้วยเหตุนี้ ประเทศสหราชอาณาจักรได้วางบทบัญญัติเพื่อบังคับใช้กับความผิดฐานฟอกเงิน ซึ่งได้กำหนดไว้ในพระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The

Proceeds of Crime Act,2002) ซึ่งได้กำหนดฐานความผิดเกี่ยวกับการปกปิด ปิดบัง เงิน หรือทรัพย์สินที่ได้มาหรือได้ประโยชน์มาจากการกระทำความผิด และในปัจจุบันการโอนเงินทางอิเล็กทรอนิกส์เป็นวิธีการหนึ่งที่เป็นที่นิยมในการปกปิด หรือปิดบังเงินหรือทรัพย์สินที่ได้มาหรือได้ประโยชน์มาจากการกระทำความผิด ซึ่งทำให้การฟอกเงินอาจเป็นความผิดหนึ่งที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ทั้งนี้ หากพิจารณาถึงพระราชบัญญัติแต่ละฉบับมีสาระสำคัญดังนี้

3.2.2.1 พระราชบัญญัติการกระทำโดยมิชอบต่อคอมพิวเตอร์ ค.ศ. 1990 (The Computer Misuse Act,1990)

ด้วยเหตุนี้ หากพิจารณาถึงมาตรการทางกฎหมายแห่งประเทศสหราชอาณาจักรในการกำหนดลักษณะความผิดเกี่ยวกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งได้กำหนดไว้ในพระราชบัญญัติการกระทำโดยมิชอบต่อคอมพิวเตอร์ ค.ศ.1990 (The Computer Misuse Act,1990) ตามบทบัญญัติแห่งกฎหมายฉบับดังกล่าวได้กำหนดฐานความผิดเพื่อใช้บังคับกับการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ไว้โดยเฉพาะ ซึ่งย่อมรวมถึงอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ด้วย ไม่ว่าจะเป็น "การเข้าถึง" หรือ "การเข้าถึงโดยปราศจากอำนาจ" หรือ "แก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์ และส่วนประกอบของคอมพิวเตอร์โดยปราศจากอำนาจ" โดยกฎหมายดังกล่าวได้บัญญัติถึงลักษณะความผิดทางคอมพิวเตอร์ ซึ่งมีสาระสำคัญ ดังนี้

3.2.2.1.1 ความผิดฐาน "การเข้าถึงโดยปราศจากอำนาจ"

ความผิดของ "การเข้าถึงโดยปราศจากอำนาจ" ได้บัญญัติไว้ใน The Computer Misuse Act 1990 มาตรา 1[51] โดยมีองค์ประกอบความผิด กล่าวคือ

1. ผู้ใดบุคคลได้กระทำการให้คอมพิวเตอร์แสดงผล หรือแสดงการทำงานใดๆ ด้วยเจตนาที่จะผ่านสิ่งป้องกันที่มีไว้เพื่อป้องกันการเข้าถึงระบบ และทำการผ่านสิ่งป้องกันเช่นว่านั้นเข้าถึงโปรแกรมคอมพิวเตอร์ใดๆ หรือสารสนเทศที่เก็บไว้ในคอมพิวเตอร์ใดๆ

---

[51] Computer Misuse Act, section 1.

1.1 โดยการผ่านสิ่งป้องกันเข้าไปยังระบบนั้น เป็นการกระทำโดยปราศจากอำนาจ

1.2 บุคคลนั้นรู้ขณะที่กระทำอยู่แล้วว่า การกระทำอันเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานนั้นปราศจากอำนาจ

2. เจตนาของบุคคลที่ได้กระทำความผิดภายใต้มาตรานี้ไม่จำเป็นต้องมีการกระทำที่เป็น

2.1 โปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล

2.2 โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือ

2.3 โปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ

บทกำหนดโทษ

ผู้กระทำความผิดตามมาตรานี้ และต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐาน หรือทั้งจำทั้งปรับ

หากพิจารณาถึงบทบัญญัติแห่งฉบับนี้จะเห็นได้ว่า เป็นกฎหมายพื้นฐานที่กำหนดความผิดต่อการกระทำอันเป็นการเข้าถึงข้อมูลโดยปราศจากอำนาจ โดยกฎหมายดังกล่าวมุ่งเน้นผลแห่งการกระทำแต่มิได้กำหนดลักษณะของการกระทำความผิดไว้แต่อย่างใดๆ กล่าวคือ

ประการแรก ความผิดลักษณะดังกล่าวมิได้กำหนดว่าบุคคลหนึ่งบุคคลใดได้กระทำการในลักษณะหนึ่งลักษณะใดให้เป็นความผิดเช่นความผิดในลักษณะเดียวกันนี้ หากแต่กฎหมายดังกล่าวกำหนดไว้อย่างกว้างๆ โดยรวมว่า บุคคลหนึ่งบุคคลใดได้กระทำการอันทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานโดยผ่านจากสิ่งที่ป้องกันของระบบดังกล่า และไม่จำเป็นว่าการกระทำดังกล่าวได้กระทำไปเพื่อประโยชน์อย่างใดหรือไม่ ดังนั้นการพิจารณากฎหมายดังกล่าวจะเห็นว่าองค์ประกอบของความผิดแห่งความผิดสำเร็จตามกฎหมายฉบับนี้ คือ การกระทำใดๆ อันทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงาน โดยผ่านสิ่งป้องกันอย่างหนึ่งอย่างใดถือเป็นความผิดตามกฎหมายฉบับนี้แล้ว

ประการที่สอง หากพิจารณาถึงองค์ประกอบภายใน หรือเจตนาภายในของผู้กระทำความผิดตามกฎหมายฉบับนี้ที่ได้กำหนดไว้ กล่าวคือ

1. กำหนดให้ผู้กระทำความผิดเจตนาผ่านสิ่งป้องกันที่มีไว้ในระบบ กล่าวคือ เจตนาเข้าสู่ระบบ และไม่จำเป็นต้องมุ่งหมายกระทำการต่อโปรแกรมใดโปรแกรมหนึ่งโดยเฉพาะ หากแต่บุคคลดังกล่าวได้กระทำการอย่างหนึ่งอย่างใดอันเป็นการเข้าสู่ระบบคอมพิวเตอร์ได้ย่อมถือเป็นความผิดดังกล่าวแล้ว
2. กำหนดให้ผู้กระทำความผิดซึ่งได้รู้ขณะซึ่งกระทำการให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานโดยปราศจากอำนาจดังกล่าว ซึ่งแสดงถึงเจตนาอันจงใจในการเข้าสู่ระบบให้เพื่อคอมพิวเตอร์แสดงการทำงานอย่างหนึ่งอย่างใด

ประการที่สาม กระบวนวิธีพิจารณาคดีตามที่มาตรานี้ได้กำหนดให้มีลักษณะพิเศษโดยความผิดในการเข้าถึงโดยปราศจากอำนาจนี้ ต้องมีการพิจารณาคดีที่รวบรัดตามกระบวนวิธีพิจารณาแห่งสหราชอาณาจักร ซึ่งพิจารณาแล้วจะเห็นว่าการกำหนดให้ความผิดในลักษณะดังกล่าวมีการพิจารณาคดีโดยรวบรัด ด้วยเหตุว่าพยานหลักฐานทางอิเล็กทรอนิกส์มีลักษณะพิเศษที่สามารถแก้ไข เปลี่ยนแปลง หรือทำลายได้โดยง่าย และการกระทำต่อระบบอิเล็กทรอนิกส์สามารถสร้างความเสียหายได้อย่างรวดเร็ว ทั้งนี้ การกำหนดให้มีการพิจารณาคดีโดยรวบรัดจึงมีความจำเป็น และเป็นประโยชน์ในการคุ้มครองพยานหลักฐานทางอิเล็กทรอนิกส์ และสามารถป้องกันความเสียหายที่อาจเกิดขึ้นจากการกระทำความผิดดังกล่าว

หากพิจารณาถึงบทกำหนดโทษของความผิดที่กระทำต่อคอมพิวเตอร์ที่กำหนดไว้ในกฎหมายฉบับนี้จะเห็นได้ว่ามิได้มุ่งเน้นในการลงโทษจำคุกแก่ผู้กระทำความผิด หากแต่กฎหมายฉบับนี้มุ่งเน้นบทกำหนดโทษทางแพ่ง หรือวิธีการเพื่อความปลอดภัยในการบังคับใช้กับกรณีดังกล่าวมากกว่า และแม้ว่ากฎหมายฉบับดังกล่าวจะสามารถบังคับใช้กับการกระทำความผิดอันเป็นการเข้าถึงข้อมูลในการโอนเงินทางอิเล็กทรอนิกส์ แต่กฎหมายฉบับดังกล่าวไม่อาจใช้บังคับให้ครอบคลุมถึงกรณีแห่งการกระทำอันเป็นความผิดในการโอนเงินทางอิเล็กทรอนิกส์ในลักษณะอื่นๆ ได้ กฎหมายสามารถบังคับได้เพียงการกระทำที่กระทำต่อระบบคอมพิวเตอร์เท่านั้น

3.2.2.1.2 ความผิดฐานการเข้าถึงโดยปราศจากอำนาจ เพื่อให้ความสะดวกหรือส่งเสริมในการกระทำความผิดดังกล่าว

ความผิดของ "การเข้าถึงโดยปราศจากอำนาจโดยมีเจตนาในการให้ความสะดวกหรือส่งเสริมการกระทำความผิด" ได้บัญญัติไว้ใน The Computer Misuse Act 1990 มาตรา 2[52] โดยมีสาระสำคัญดังนี้

1. ผู้ใดเจตนาได้กระทำความผิดที่กฎหมายนี้ได้บัญญัติไว้ เพื่อให้ความสะดวกในการกระทำความผิด (ไม่ว่าจะเป็นความสะดวกของตนเองหรือของบุคคลอื่นๆ) โดยการกระทำการดังกล่าวข้างต้นให้ถือว่าเสมือนเป็นผู้กระทำความผิด เช่นเดียวกับผู้กระทำความผิดที่บุคคลนั้นได้เข้าไปช่วย
2. ผู้ใดเจตนาได้กระทำความผิดที่กฎหมายนี้ได้บัญญัติไว้ และเป็นบุคคลที่มีอายุตั้งแต่ 21 ปีขึ้นไป
3. ผู้ใดกระทำการให้เป็นไปตามวัตถุประสงค์ในการกระทำความผิดตามที่กฎหมายนี้ได้บัญญัติไว้โดยอาศัยโอกาสทางธุรกิจ หรือเพื่อกระทำความผิดดังกล่าวล่วงหน้า

<u>บทกำหนดโทษ</u>

1. บุคคลที่มีความผิดตามมาตรานี้ ซึ่งเป็นคดีที่ดำเนินคดีแบบรวบรัด ผู้นั้นอาจต้องรับผิดในโทษปรับสูงสุด หรือจำคุกไม่เกิน หก เดือน หรือทั้งจำทั้งปรับ ตามมาตรา 2 (5)(a)
2. บุคคลที่มีความผิดตามมาตรานี้ ซึ่งเป็นคดีสามัญทั่วไป บุคคลนั้นอาจต้องรับผิดอัตราโทษปรับสูงสุด หรือจำคุก ไม่เกิน ห้า ปี หรือทั้งจำทั้งปรับ ตามมาตรา 2 (5)(b)
3. หากบุคคลนั้นมีอายุตั้งแต่ 21 ปีขึ้นไปโดยบุคคลนั้นอาจต้องรับผิดในอัตราโทษปรับสูงสุด หรือจำคุก ไม่เกิน ห้า ปี หรือทั้งจำทั้งปรับ ตามมาตรา 2 (2)(b) และ
4. หากการกระทำความผิดดังกล่าวได้กระทำโดยอาศัยโอกาสทางธุรกิจ บุคคลนั้นอาจมีโทษปรับตามสมควรหรือเท่าที่เป็นไปได

---

[52] <u>Computer Misuse Act</u>, section 2.

ทั้งนี้ หากพิจารณาถึงมาตรา 2 นี้จะเห็นได้ว่าวัตถุประสงค์แห่งมาตรานี้มุ่งบังคับใช้กับผู้กระทำความผิดที่อาจมิได้ลงมือกระทำความผิดโดยตรง หรือไม่มีโอกาสกระทำความผิดโดยตรง โดยเป็นผู้สนับสนุนหรือให้ความสะดวกอย่างหนึ่งอย่างใด กฎหมายฉบับนี้สามารถบังคับใช้กับบุคคลที่มิได้ลงมือกระทำความผิดดังกล่าว แต่หากมีเจตนาช่วยให้ความสะดวกหรือส่งเสริมในการกระทำความผิดก็ให้ถือว่ามีความผิดตามมาตรานี้ ดังนั้น ความผิดฐานการเข้าถึงโดยปราศจากอำนาจ และเป็นการกระทำไปเพื่อสนับสนุน ส่งเสริมการกระทำความผิดจึงถือว่าเป็นความผิดที่บังคับใช้กับบุคคลซึ่งเป็นผู้สนับสนุน ส่งเสริม หรือให้ความสะดวกในการกระทำความผิด และต้องรับผิดตามมาตรา 2 แห่งบทบัญญัติฉบับนี้

3.2.2.1.3 ความผิดฐาน "แก้ไขเปลี่ยนแปลง เครื่องคอมพิวเตอร์ และส่วนประกอบของคอมพิวเตอร์โดยปราศจากอำนาจ"

ความผิดของ "การแก้ไขเปลี่ยนแปลงโดยปราศจากอำนาจ" ได้บัญญัติไว้ใน The Computer Misuse Act 1990 มาตรา 3[53] โดยมีสาระสำคัญดังนี้

1. บุคคลใดซึ่งกระทำการใดๆ อันเป็นการก่อให้เกิดการแก้ไขเปลี่ยนแปลงสิ่งที่บรรจุอยู่ในคอมพิวเตอร์ใดๆ และกระทำโดยเจตนาและจำเป็นต้องรู้ถึงการกระทำนั้น
2. วัตถุประสงค์ของเจตนาในข้อ (1) หมายถึง เจตนาที่จะก่อให้เกิดการแก้ไขเปลี่ยนแปลงสิ่งที่บรรจุอยู่ในคอมพิวเตอร์ใดๆ และกระทำโดย
   2.1 การทำให้เสียไป ซึ่งการปฏิบัติการของคอมพิวเตอร์นั้น
   2.2 การป้องกันหรือขัดขวางต่อการเข้าถึงโปรแกรมหรือข้อมูลใดๆ ขอเครื่องคอมพิวเตอร์
   2.3 ทำให้เสียไป ซึ่งระบบในการปฏิบัติการของโปรแกรมของคอมพิวเตอร์ หรือความน่าเชื่อถือของโปรแกรมคอมพิวเตอร์
3. โดยเจตนาดังกล่าวไม่จำเป็นต้องกระทำโดยตรงต่อ
   3.1 คอมพิวเตอร์ใดๆ โดยเฉพาะ
   3.2 ข้อมูลหรือโปรแกรมเฉพาะหรือข้อมูล หรือโปรแกรมชนิดใดชนิดหนึ่ง

---

[53] Computer Misuse Act, section 3.

3.3 การแก้ไขเปลี่ยนแปลงใดๆ โดยเฉพาะหรือการแก้ไขซึ่งอย่างหนึ่งอย่างใดโดยเฉพาะ

4. วัตถุประสงค์ของในการใช้บังคับกรณีที่กำหนดไว้ในข้อ 1. นั้น ผู้กระทำนั้นไม่จำเป็นต้องรู้ถึงการกระทำนั้น หมายถึง การได้รู้ถึงผลแห่งการเปลี่ยนแปลงนั้น หากแต่ผู้นั้นได้เจตนาเปลี่ยนแปลงโดยปราศจากอำนาจตามข้อ 1. เช่นนี้ ก็ถือได้ว่าเป็นความผิดตามมาตรานี้แล้ว

5. วัตถุประสงค์ของมาตรานี้ให้ใช้บังคับถึงส่วนประกอบ หรืออุปกรณ์ใดๆของคอมพิวเตอร์ ไม่ว่าการแก้ไขเปลี่ยนแปลงดังกล่าวจะเป็นการเปลี่ยนแปลงโดยถาวร หรือเพียงชั่วคราวก็ตาม

6. การแก้ไขเปลี่ยนแปลง ซึ่งสิ่งที่บรรจุอยู่ในคอมพิวเตอร์ โดยปกติจะถือว่าได้รับการคุ้มครองในการชดเชยความเสียหายตามพระราชบัญญัติความเสียหายจากอาชญากรรม (Criminal Damage Act) ถ้าการกระทำส่งผลกระทบโดยตรงต่อคอมพิวเตอร์ สื่อบันทึกใดๆ ของคอมพิวเตอร์ อันเป็นการทำให้เสียไป ไม่ว่าจะเป็นความเสียไปทางด้านในเงื่อนไขต่างๆ หรือความเสียไปของสิ่งนั้น

<u>บทกำหนดโทษ</u>

1. บุคคลที่มีความผิดตามมาตรานี้ และเป็นคดีที่ดำเนินคดีแบบรวบรัด บุคคลนั้นอาจต้องรับผิดในโทษปรับสูงสุด หรือจำคุก ไม่เกินหก เดือน หรือทั้งจำทั้งปรับ

2. บุคคลที่มีความผิดตามมาตรานี้ และเป็นคดีที่ดำเนินคดีสามัญทั่วไป บุคคลนั้นอาจต้องรับผิดในอัตราโทษปรับสูงสุด หรือจำคุกไม่เกินห้า ปี หรือทั้งจำทั้งปรับ แล้วแต่กรณี

ทั้งนี้ หากพิจารณาถึงความผิดตามบทบัญญัติฉบับนี้ที่ได้อธิบายข้างต้นกับการกำหนดลักษณะการกระทำความผิดที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ยังมีข้อควรพิจารณาหลายประการ กล่าวคือ

ประการแรก บทบัญญัติดังกล่าวได้บัญญัติลักษณะของการกระทำความผิดฐาน "การเข้าถึงโดยปราศจากอำนาจ" หรือ "การเข้าถึงโดยปราศจากอำนาจเพื่ออำนวยความสะดวกแก่การกระทำความผิด" หรือ "การแก้ไขเปลี่ยนแปลงต่อเครื่องคอมพิวเตอร์หรือสื่ออุปกรณ์ใดของเครื่องคอมพิวเตอร์"ซึ่งเป็นการกำหนดฐานลักษณะฐานความผิดทางคอมพิวเตอร์อย่างกว้างๆ ไว้เพื่อให้สามารถใช้บังคับกับอาชญากรรมทางคอมพิวเตอร์ได้ในทุกกรณี ดังนั้นความผิดในแต่ละฐานความผิดดังกล่าว จึงสามารถนำมาปรับใช้กับการกระทำความผิดที่มีลักษณะเป็นอาชญากรรมทางคอมพิวเตอร์ที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ได้

ประการที่สอง การกำหนดบทกำหนดโทษตามแต่ละฐานความผิดแห่งพระราชบัญญัติฉบับนี้มีลักษณะพิเศษ เพื่อให้สามารถกำหนดบทลงโทษที่เหมาะสมกับความผิดในแต่ละลักษณะได้ [54] กล่าวคือ

1. บุคคลที่มีความผิดตามมาตรานี้ ซึ่งเป็นคดีที่มีการดำเนินคดีแบบรวดรัด บุคคลนั้นมีโทษจำคุกไม่เกิน หก เดือน หรือโทษปรับสูงสุด หรือทั้งจำทั้งปรับ ซึ่งโทษปรับสูงสุดกรณีดังกล่าวเป็นโทษปรับไม่เกิน 2,000 ปอนด์
2. บุคคลที่มีความผิดตามมาตรานี้ ซึ่งเป็นคดีที่มีการดำเนินคดีโดยสามัญทั่วไป บุคคลนั้นมีโทษจำคุกไม่เกิน ห้า ปี หรือโทษปรับสูงสุด หรือทั้งจำทั้งปรับ ซึ่งโทษปรับสูงสุดกรณีดังกล่าวไม่จำกัดอัตราโทษปรับสูงสุดไว้

ประการที่สาม หากเป็นกรณีผู้กระทำความผิดได้กระทำความผิดโดยอาศัยโอกาสทางธุรกิจ ผู้กระทำความผิดต้องรับผิดในอัตราโทษจำคุก หรือโทษปรับสูงสุด ซึ่งบทบัญญัติดังกล่าวยังไม่ได้จำกัดอัตราโทษปรับไว้ และให้ใช้ดุลยพินิจของศาลปรับตามเห็นสมควรหรือเท่าที่เป็นไปได้

ประการที่สี่ ความผิดต่อการแก้ไขเปลี่ยนแปลงต่อเครื่องคอมพิวเตอร์หรือสื่ออุปกรณ์ใดๆ ของเครื่องคอมพิวเตอร์ โดยมีมาตรการพิเศษในการคุ้มครองการชดเชยความเสียหายในกรณีดังกล่าวให้แก่ผู้เสียหาย โดยมิได้มุ่งหมายเพียงในการกำหนดบทลงโทษผู้กระทำความผิดเท่านั้น

---

[54] Neil Morris, The Summary of The Computer Misuse Act 1990. (UKERNA TEAM)[online] Available from : http://www.mcc.ac.uk/cos/security/CMA_summary.html.

3.2.2.2 พระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ.2002 (The Proceeds of Crime Act,2002)

ประเทศสหราชอาณาจักรเป็นศูนย์กลางทางการเงินการธนาคารของสหภาพยุโรป โดยเฉพาะกรุงลอนดอนซึ่งเป็นศูนย์กลางการค้าการแลกเปลี่ยนเงินตราต่างประเทศที่ใหญ่ที่สุด และมีธนาคารต่างประเทศมากกว่า 100 สาขา ซึ่งร้อยละ 83 เป็นธนาคารของกลุ่มประเทศในสหภาพยุโรป[55] ประกอบกับองค์กรอาชญากรรมหรืออาชญากรทางเศรษฐกิจในปัจจุบันได้เริ่มนิยมใช้โอกาสจากระบบการเงินการธนาคารหรือการโอนเงินทางอิเล็กทรอนิกส์ที่มีความสะดวกและรวดเร็วมาเป็นเครื่องมือในการฟอกเงินมากยิ่งขึ้น

ด้วยเหตุนี้ พระราชบัญญัติฉบับนี้จึงได้วางบทบัญญัติในการบังคับใช้กับความผิดฐานฟอกเงิน เพื่อคุ้มครองระบบการเงินการธนาคารให้มีความปลอดภัยและสามารถบังคับใช้กับความผิดฐานฟอกเงินดังกล่าวได้อย่างมีประสิทธิภาพ ด้วยแต่เดิมความผิดฐานฟอกเงินมักจะบังคับใช้เพียงเงินที่ได้มา หรือได้ประโยชน์จากความผิดเกี่ยวกับยาเสพติด แต่ปัจจุบันพระราชบัญญัติฉบับนี้ไม่ได้จำกัดให้ใช้บังคับเฉพาะเงิน หรือทรัพย์สินที่ได้มาหรือได้ประโยชน์หรือใช้ในการกระทำความผิดเกี่ยวกับยาเสพติดเท่านั้น แต่สามารถบังคับใช้กับเงินที่มีที่มา หรือได้ประโยชน์ หรือใช้ในการกระทำความผิดลักษณะอื่นๆ ได้ ซึ่งพระราชบัญญัติฉบับนี้ได้กำหนดลักษณะความผิดฐานฟอกเงินซึ่งเป็นความผิดหลักอยู่ทั้งหมด 3 ลักษณะความผิด[56] กล่าวคือ

1. ความผิดฐานปกปิด (Concealing) โดยกำหนดให้ผู้ใดกระทำความผิดโดยการปกปิด ปิดบัง เปลี่ยนแปลงหรือโอนทรัพย์สินที่ได้มาจากการกระทำความผิด ณ ส่วนใดส่วนหนึ่งของประเทศสหราชอาณาจักร หรือทรัพย์สินที่เป็นเครื่องมือในการกระทำความผิด
2. ความผิดฐานการจัดการ (Arrangement) โดยกำหนดให้ผู้ใดกระทำความผิดโดยการจัดการทรัพย์สิน เพื่ออำนวยความสะดวกในการประกอบอาชญากรรม การจัดการ หรือการควบคุมทรัพย์สินที่ได้มาจากการประกอบอาชญากรรม

---

[55] UK : The financial Capital of EUROPE. [online] Available from : http://www.investuk-usa.com.

[56] Money Laundering and the Proceeds of Crime Act 2002. [online] Available from : http//www.legal500.com/devs/uk/cc/ukcc_002.html.

3. ความผิดฐานต่อการให้ได้มา การใช้ และการดำเนินอาชญากรรม (Acquisition , use and possession) โดยกำหนดให้ผู้กระทำความผิดโดยรู้ว่าทรัพย์สินดังกล่าว ได้มา ใช้ หรือเป็นส่วนหนึ่งของการดำเนินอาชญากรรมนั้นเจตนาปกปิด หรือปิดบังการรายงานต่อพนักงานเจ้าหน้าที่ที่มีอำนาจในการแก้ไขปัญหาดังกล่าว

<u>บทกำหนดโทษ</u>

ผู้ใดกระทำความผิดฐานฟอกเงินตามที่ได้กำหนดไว้ใน 3 ลักษณะความผิดข้างต้น พระราชบัญญัติฉบับนี้ได้กำหนดให้ถือว่าผู้นั้นมีความผิดทางอาญา และมีโทษปรับอัตราสูงสุดหรือจำคุกไม่เกิน 14 ปี หรือทั้งจำทั้งปรับ

3.2.3 สหภาพยุโรป (European Union)

หากพิจารณาถึง มาตรการทางกฎหมายในการกำหนดลักษณะความผิดเกี่ยวกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งคณะกรรมาธิการแห่งสภาสหภาพยุโรปได้มีการบัญญัติฐานความผิดต่างๆ เกี่ยวกับคอมพิวเตอร์ไว้ในอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ ซึ่งมุ่งหมายให้ลักษณะของความผิดที่กำหนดไว้ในอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์เป็นแนวทางในการกำหนดลักษณะความผิดของอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งสาระสำคัญของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ได้กำหนดไว้ดังต่อไปนี้

<u>อนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์แห่งสภาสหภาพยุโรป</u>
<u>(Convention on Cybercrime)</u>

คณะกรรมาธิการแห่งสภาสหภาพยุโรป ได้ร่วมกันพิจารณาอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ขึ้น เพื่อวัตถุประสงค์ในการบรรลุความสำเร็จในความร่วมมือระหว่างประเทศของกลุ่มประเทศสมาชิกแห่งสหภาพยุโรป เมื่อวันที่ 23 พฤศจิกายน 2544 (20 November 2001) ซึ่งอนุสัญญาดังกล่าวเป็นการสนับสนุนให้มีการกำหนดกฎเกณฑ์หรือแนวทางที่บังคับใช้กับอาชญากรรมคอมพิวเตอร์ไว้โดยเฉพาะ เพื่อการบังคับใช้กฎหมายกับอาชญากรรมทางคอมพิวเตอร์ภายในประเทศสมาชิกเป็นไปได้อย่างมีประสิทธิภาพ โดยอนุสัญญาดังกล่าวถือเป็นข้อตกลงร่วมกันว่า “ประเทศสมาชิกต้องปรับปรุงกฎหมายหรือมาตรการทางกฎหมายอันจำเป็น เพื่อการ

บังคับใช้กับการกระทำความผิดใดๆ ตามอนุสัญญานี้กำหนดไว้ให้เป็นความผิดถือว่าเป็นความผิดต่อกฎหมายภายในด้วย"

และหากพิจารณาถึง ความสัมพันธ์ระหว่างการโอนเงินทางอิเล็กทรอนิกส์กับความผิดตามอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ จะเห็นได้ว่าอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ได้กำหนดให้ การบังคับใช้กฎหมายดังกล่าวสามารถครอบคลุมถึงอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ได้ เนื่องจาก คำนิยามของคำว่า "ระบบคอมพิวเตอร์" และ "ข้อมูลคอมพิวเตอร์" ที่กำหนดไว้ในในมาตรา 1[57] ซึ่งได้กำหนดว่า

"ระบบคอมพิวเตอร์" หมายถึง เครื่องอิเล็กทรอนิกส์ หรือกลุ่มอุปกรณ์ในการเชื่อมต่อกับเครื่องอิเล็กทรอนิกส์อย่างใดอย่างหนึ่ง หรือทั้งหมดเพื่อการปฏิบัติงานของโปรแกรมหรือการดำเนินการใดๆ ต่อข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายถึง ข้อเท็จจริงที่แสดงออก หรือข้อมูลหรือแนวทางที่เป็นไปได้ในการดำเนินงานของระบบคอมพิวเตอร์ รวมถึงความสมบูรณ์ของโปรแกรมในการดำเนินงานของระบบคอมพิวเตอร์หรือในการทำหน้าที่ต่างๆ ของคอมพิวเตอร์

อย่างไรก็ตาม หากพิจารณาถึงคำนิยามของคำว่า "ระบบคอมพิวเตอร์" และ "ข้อมูลทางคอมพิวเตอร์" ดังกล่าวจะเห็นได้ว่าสามารถตีความให้ครอบคลุมถึงระบบโอนเงินทางอิเล็กทรอนิกส์ทางการเงินการธนาคารได้ ดังนั้นอนุสัญญาฉบับดังกล่าวจึงถือได้ว่าเป็นแนวทางด้านกฎหมายในการวางมาตรการให้ประเทศสมาชิกต้องคำนึงถึงบทบัญญัติอันเป็นความผิดต่อการเข้าถึงระบบคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ไว้ด้วย ซึ่งอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ได้กำหนดลักษณะของแต่ละฐานความผิดไว้ โดยมีสาระสำคัญดังนี้

1. การเข้าถึงโดยผิดกฎหมาย (Illegal Access)

ตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ มาตรา 2[58] ได้กำหนดความผิดลักษณะนี้ว่า การกระทำใดๆ โดยเจตนากระทำการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือ

---

[57] Convention on Cybercrime,article 1. [online] Available from : http://www.conventions.coe.int.

[58] Ibid., article 2.

แต่บางส่วนโดยปราศจากสิทธิ และมุ่งหมายให้ได้รับข้อมูลทางคอมพิวเตอร์โดยเจตนาทุจริตต่อระบบคอมพิวเตอร์ หรือทุจริตการเชื่อมต่อคอมพิวเตอร์อีกเครื่องหนึ่งนั้น นอกจากนั้นความผิดฐานเข้าถึงโดยผิดกฎหมายดังกล่าวต้องถือว่าเป็นการกระทำอันละเมิดต่อมาตรการความปลอดภัย

2. การดักฟังข้อมูลโดยมิชอบด้วยกฎหมาย (Illegal Interception)

ตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ มาตรา 3[59] ได้กำหนดความผิดลักษณะนี้ว่า การกระทำใดๆ โดยเจตนาดักฟังระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนโดยปราศจากสิทธิ และการกระทำดังกล่าวเป็นการกระทำต่อเทคโนโลยี การโอนข้อมูลส่วนบุคคลจากระบบคอมพิวเตอร์หรือข้อมูลที่อยู่ในระบบคอมพิวเตอร์ ณ ที่หนึ่งที่ใด รวมถึงคำสั่งทางการเงินผ่านแถบแม่เหล็กที่ส่งผ่านระบบคอมพิวเตอร์ โดยมีวัตถุประสงค์ในการดักฟังข้อมูลทางคอมพิวเตอร์ หรือเจตนาทุจริตต่อระบบคอมพิวเตอร์ หรือเจตนาทุจริตต่อการเชื่อมต่อกับคอมพิวเตอร์เครื่องหนึ่งกับคอมพิวเตอร์อีกเครื่องหนึ่งก็ได้

3. การรบกวนข้อมูล (Data Interference)

ตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ มาตรา 4[60] (Convention on Cybercrime Article 4) ได้กำหนดความผิดลักษณะนี้ว่า การกระทำใดๆ โดยเจตนากระทำการอันเป็นการทำให้เสียหาย ทำลาย ทำให้เสื่อมลง การเปลี่ยนแปลง การระงับซึ่งข้อมูลของคอมพิวเตอร์โดยปราศจากสิทธิ

4. การรบกวนระบบ (System Interference)

ตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ มาตรา 5[61] ได้กำหนดความผิดในลักษณะนี้ว่า การกระทำใดๆ โดยเจตนากระทำการอันเป็นการขัดขวางการทำงานของระบบคอมพิวเตอร์ หรือการทำหน้าที่ของคอมพิวเตอร์อย่างร้ายแรงโดยปราศจากสิทธิ โดยการ

---

[59] Convention on Cybercrime., article 3. [online] Available from : http://www.conventions.coe int.

[60] Ibid., article 4.

[61] Ibid., article 5.

กระทำการใส่ เคลื่อนย้าย ทำให้เสียหาย ทำลาย ทำให้เสื่อมลง การเปลี่ยนแปลง หรือการระงับซึ่งข้อมูลทางคอมพิวเตอร์

5. การใช้เครื่องหรืออุปกรณ์ทางอิเล็กทรอนิกส์โดยมิชอบ (Misuse of Devices)

ตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ มาตรา 6[62] ได้กำหนดความผิดลักษณะนี้ว่า การกระทำใดๆ โดยเจตนาและปราศจากสิทธิต่อการกระทำต่อไปนี้

1. การสร้าง ขาย ล่อลวงในการใช้ นำเข้า จำแนก หรือการกระทำโดยวิธีหนึ่งวิธีใด โดยเป็นการกระทำต่อ
   1.1 เครื่องอิเล็กทรอนิกส์ โปรแกรมคอมพิวเตอร์ หรือการออกแบบ หรือการปรับปรุงเบื้องต้นเพื่อให้เป็นไปตามวัตถุประสงค์ในการกระทำความผิดในข้อ 1 ข้อ 2 ข้อ 3 หรือ ข้อ 4 ซึ่งได้อธิบายแล้วข้างต้น
   1.2 รหัสผ่านคอมพิวเตอร์ รหัสการเข้าถึง ข้อมูลที่มีลักษณะเช่นนั้น เพื่อการเข้าถึงระบบคอมพิวเตอร์ไม่ว่าทั้งหมดหรือบางส่วน และมีเจตนาในการใช้ตามวัตถุประสงค์ในการกระทำความผิดในข้อ 1 ข้อ 2 ข้อ 3 หรือ ข้อ 4 ซึ่งได้อธิบายแล้วข้างต้น

2. โดยมีวัตถุประสงค์เพื่อการครอบครองเครื่องอิเล็กทรอนิกส์ โปรแกรมคอมพิวเตอร์ หรือการออกแบบตามวัตถุประสงค์ในการกระทำความผิดในข้อ 1 ข้อ 2 ข้อ 3 หรือ ข้อ 4 และรหัสผ่านคอมพิวเตอร์ รหัสการเข้าถึง ข้อมูลที่มีลักษณะเช่นนั้น เพื่อการเข้าถึงระบบคอมพิวเตอร์ไม่ว่าทั้งหมดหรือบางส่วน โดยมีวัตถุประสงค์ในการกระทำความผิดตามที่ได้กำหนดไว้ในข้อ 1 ข้อ 2 ข้อ 3 หรือ ข้อ 4 ข้างต้น

3. การกำหนดความรับผิดทางอาญาในมาตรานี้ต้องเป็นการกระทำใดๆ ที่มีวัตถุประสงค์ในการกระทำความผิด หรือการใช้เครื่องหรืออุปกรณ์ทาง

---

[62] Convention on Cybercrime, article 6. [online] Available from : http://www.conventions.coe.int.

อิเล็กทรอนิกส์โดยมิชอบ (Misuse of Devices) โดยมีวัตถุประสงค์ในการกระทำความผิดตามข้อ 1 ข้อ 2 ข้อ 3 หรือ ข้อ 4 ข้างต้น

6. ความผิดที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ (Computer-related offences)

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ มาตรา 7[63] ได้กำหนดความผิดลักษณะนี้ว่า การกระทำใดๆ โดยเจตนาและปราศจากสิทธิในการใส่ เปลี่ยนแปลง การทำลาย หรือการระงับข้อมูลคอมพิวเตอร์ หรือการทำให้ผลของข้อมูลที่ผิดไปจากความจริง ซึ่งรวมถึงการกระทำเจตนาในการฉ้อโกง หรือเจตนาทุจริตในการกระทำกรณีดังกล่าวด้วย

7. ความผิดที่เกี่ยวข้องกับการฉ้อโกงทางคอมพิวเตอร์ (Computer-related forgery)

ตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ มาตรา 8[64] ได้กำหนดความผิดลักษณะนี้ว่า การกระทำใดๆ โดยเจตนาและปราศจากสิทธิอันเป็นเหตุให้สูญเสียทรัพย์สินอย่างหนึ่งอย่างใด โดยการ

1. ใส่ เปลี่ยนแปลง การทำลาย หรือการระงับข้อมูลคอมพิวเตอร์
2. การแทรกแซงหน้าที่การทำงานของระบบคอมพิวเตอร์
3. โดยเจตนาหลอกลวง หรือเจตนาทุจริตเพื่อการล่อลวง หรือการกระทำโดยปราศจากสิทธิ หรือเพื่อผลประโยชน์ต่อตนเองหรือบุคคลอื่น”

<u>บทกำหนดโทษ</u>

1. รับผิดทางแพ่ง

ตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ มาตรา 12[65] ได้กำหนดให้ ประเทศสมาชิกต้องปรับปรุงกฎหมายหรือมาตรการอันจำเป็นในการผูกพันต่อนิติบุคคล

---

[63] Convention on Cybercrime,. article7. [online] Available from : http://www.conventions.coe.int.

[64] Ibid., article 8.

โดยประเทศสมาชิกต้องกำหนดความรับผิดในลักษณะความผิดต่างๆ ข้างต้น ไม่ว่าจะเป็นความรับผิดทางแพ่ง ความรับผิดทางอาญา หรือความผิดของหน่วยงานแห่งภาครัฐอย่างใด

2. การลงโทษ

ตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ มาตรา 13[66] ได้กำหนดให้ในแต่ละความผิดตามอนุสัญญาดังกล่าวต้องกำหนดมาตรการในการลงโทษการกระทำความผิดในแต่ละลักษณะความผิดไว้ กล่าวคือ

1. ประเทศสมาชิกจะต้องปรับปรุงกฎหมายหรือมาตรการทางกฎหมายที่จำเป็นเพื่อผูกพันแก่การกระทำความผิดที่ได้อธิบายข้างต้น เพื่อการลงโทษที่มีประสิทธิภาพ และบทลงโทษดังกล่าวสามารถยับยั้งการกระทำความผิดและการลงโทษมีสัดส่วนที่เหมาะสม

2. ประเทศสมาชิกต้องกำหนดให้นิติบุคคลมีความรับผิดทางแพ่งให้แก่นิติบุคคลใดๆ โดยมีวัตถุประสงค์เพื่อการลงโทษที่มีประสิทธิภาพหรือกำหนดบทลงโทษที่สามารถยังยั้งการกระทำความผิดทางอาญาได้ รวมถึงการกำหนดบทลงโทษทางแพ่ง ซึ่งกรณีนี้หมายถึงมาตรการลงโทษทางการเงิน

นอกจากนั้น อนุสัญญาฉบับนี้ยังได้กำหนดมาตรการในการค้นและยึดข้อมูลคอมพิวเตอร์ เพื่อประโยชน์ในการรวบรวมพยานหลักฐานซึ่งกำหนดไว้ตามมาตรา 19[67] กล่าวคือ

1. ประเทศสมาชิกต้องทำการปรับปรุงบทกฎหมายและมาตรการอื่นใดที่จำเป็นและให้อำนาจแก่พนักงานเจ้าหน้าที่ในการค้น หรือการเข้าถึงข้อมูลทางอิเล็กทรอนิกส์ต่อระบบคอมพิวเตอร์ส่วนใดส่วนหนึ่งหรือ

---

[65] Convention on Cybercrime,. article 12. [online] Available from : http://www.conventions.coe.int.

[66] Ibid., article 13.

[67] Ibid, article 19.

ข้อมูลทางคอมพิวเตอร์ทั้งหมด รวมถึงการเก็บรักษาข้อมูลทางคอมพิวเตอร์ดังกล่าว

2. ประเทศสมาชิกต้องทำการปรับปรุงบทกฎหมายและมาตรการอื่นใดที่จำเป็นและให้อำนาจแก่พนักงานเจ้าหน้าที่ในการเข้าถึงระบบคอมพิวเตอร์โดยเฉพาะ โดยอยู่บนพื้นฐานของความเชื่อว่าข้อมูลที่เก็บรักษาไว้ในคอมพิวเตอร์นั้นเป็นข้อมูลที่ใช้ในการดำเนินการที่เชื่อว่าเป็นการกระทำความผิด และผู้ที่มีอำนาจหน้าที่สามารถเข้าไปค้นและเข้าถึงในลักษณะดังกล่าวได้
3. ประเทศสมาชิกต้องทำการปรับปรุงบทกฎหมายและมาตรการอื่นใดที่จำเป็นและให้อำนาจแก่พนักงานเจ้าหน้าที่ในการยึด หรือเก็บรักษาข้อมูลทางคอมพิวเตอร์ดังกล่าวโดยกำหนดมาตรการใน,
   3.1 การยึด หรือเก็บบันทึกระบบคอมพิวเตอร์หรือส่วนหนึ่งส่วนใดของคอมพิวเตอร์
   3.2 การทำและเก็บสำเนาของข้อมูลทางคอมพิวเตอร์เหล่านั้น
   3.3 การเก็บรักษาต้องอยู่บนพื้นฐานของความยุติธรรมของการเก็บข้อมูลทางอิเล็กทรอนิกส์ และ
   3.4 การส่งหรือเคลื่อนย้ายข้อมูลทางคอมพิวเตอร์ในการเข้าถึงระบบคอมพิวเตอร์ดังกล่าว
4. ประเทศสมาชิกต้องทำการปรับปรุงบทกฎหมายและมาตรการอื่นใดที่จำเป็นและให้อำนาจแก่พนักงานเจ้าหน้าที่ซึ่งมีความรู้ความเชี่ยวชาญเฉพาะด้านคอมพิวเตอร์ หรือหน้าที่ในการทำงาน หรือมาตรการในการปกป้องข้อมูลอย่างหนึ่งอย่างใด

อย่างไรก็ตามอนุสัญญาฉบับดังกล่าวนี้เป็นเพียงการกำหนดมาตรการทางกฎหมายอย่างกว้าง ๆ ในการบังคับใช้กับอาชญากรรมทางคอมพิวเตอร์ ด้วยเหตุนี้ อนุสัญญาฉบับดังกล่าวจึงเป็นแนวทางด้านกฎหมาย เพื่อบังคับใช้กับการกระทำความผิดหรืออาชญากรรมทางคอมพิวเตอร์ที่กระทำต่อระบบระบบโอนเงินทางอิเล็กทรอนิกส์โดยรวม

3.3 มาตรการทางกฎหมายการแก้ไขเยียวยาความเสียหายจากอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

3.3.1 ประเทศสหรัฐอเมริกา (United State)

ตามประมวลกฎหมายแห่งสหรัฐอเมริกาได้กำหนดถึงมาตรการในการแก้ไขเยียวยาความเสียหายจากการกระทำอาชญากรรมที่เกิดขึ้นไว้ในมาตรการการริบทรัพย์สิน ซึ่งแบ่งเป็นมาตรการการริบทรัพย์สินทางแพ่ง ที่สามารถริบทรัพย์สินที่เกี่ยวข้อหรือได้มาจากการกระทำความผิดได้ตั้งแต่มีเหตุต้องสงสัยว่ากระทำความผิด และพนักงานเจ้าหน้าที่ที่มีอำนาจหน้าที่ได้สืบเสาะถึงทรัพย์สินดังกล่าว เพื่อเป็นการระงับความเสียหายที่เกิดขึ้นจากอาชญากรรมดังกล่าวในเบื้องต้น หรือมาตรการการริบทรัพย์สินทางอาญาที่เป็นการริบทรัพย์สินโดยคำพิพากษาของศาล ในทรัพย์สินที่เกี่ยวข้องหรือได้มาจากการกระทำความผิดทั้งหมด และมาตรการทางกฎหมายในการริบทรัพย์สินดังกล่าวไม่มีข้อจำกัดว่าต้องเป็นทรัพย์สินที่เกี่ยวข้องหรือที่ได้มาจากการกระทำความผิดขณะกระทำความผิดเท่านั้น แต่ให้รวมถึงทรัพย์สินที่เกี่ยวข้องหรือได้มาจากการกระทำความผิดและได้ถูกนำมาใช้หรือแปรสภาพเป็นทรัพย์สินอื่นๆ ของผู้กระทำความผิด หรือของบุคคลอื่นๆ ก็ได้ ซึ่งเจ้าพนักงานผู้มีอำนาจหน้าที่ในกรณีดังกล่าวโดยเฉพาะจะเป็นผู้มีอำนาจหน้าที่ในการสืบเสาะทรัพย์สินดังกล่าว

มาตรการทางกฎหมายดังกล่าวได้ถูกบัญญัติไว้ให้ใช้บังคับกับการกระทำความผิดที่ได้บัญญัติไว้ในบทบัญญัติฉบับนี้เป็นการเฉพาะ ซึ่งล้วนแล้วแต่เป็นความผิดหนักตามประมวลกฎหมายอาญาทั้งสิ้น โดยมาตรการทางกฎหมายในการริบทรัพย์สินที่ใช้บังคับกับการกระทำความผิดตามที่ได้บัญญัติไว้ประมวลกฎหมายอาญาได้บัญญัติไว้ในหมวด 46 ว่าด้วย การริบทรัพย์สิน โดยแบ่งออกได้เป็น 2 ลักษณะ กล่าวคือ

1. การริบทรัพย์สินทางแพ่ง ตามมาตรา 981
2 การริบทรัพย์สินทางอาญา มาตรา 982

3.3.1. การริบทรัพย์สินทางแพ่ง

ตามประมวลกฎหมายสหรัฐอเมริกา ตามมาตรา 981[68] ได้กำหนดถึงมาตรการในการริบทรัพย์สินทางแพ่งไว้ ซึ่งมีสาระสำคัญดังนี้

1. ความผิดซึ่งได้บัญญัติให้ใช้มาตรการริบทรัพย์สินทางแพ่ง และเป็นอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ กล่าวคือ
   - 1.1 ความผิดต่อการให้ รับประโยชน์อย่างหนึ่งอย่างใดในการโอนเงินทางอิเล็กทรอนิกส์ตามมาตรา 215
   - 1.2 ความผิดต่อการทุจริตของพนักงานเจ้าหน้าที่ของธนาคารหรือสถาบันทางการเงินตามมาตรา 656 และมาตรา 657
   - 1.3 ความผิดต่อการฉ้อโกงบันทึก รายงาน หรือการเปลี่ยนแปลงทางบัญชีของธนาคาร หรือสถาบันการเงินหรือธนาคารรัฐบาลกลางตามมาตรา 1005 มาตรา 1006 หรือมาตรา 1007
   - 1.4 ความผิดต่อการเข้าถึงบัตร รหัส หรือสื่ออิเล็กทรอนิกส์ตามมาตรา 1029
   - 1.5 ความผิดต่อการเข้าถึงเครื่องคอมพิวเตอร์โดยปราศจากอำนาจตามมาตรา 1030
   - 1.6 ความผิดต่อการฉ้อโกงธนาคาร ตาม 1344
   - 1.7 ความผิดต่อการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ตามมาตรา 1956
   - 1.8 ความผิดต่อการสั่งให้โอนเงินทางอิเล็กทรอนิกส์เพื่อการฟอกเงินตามมาตรา 1957

2. ทรัพย์สินที่อยู่ในบังคับแห่งการริบทรัพย์สิน ได้แก่
   - 1.1 ทรัพย์สินใดๆ ซึ่งเป็นทรัพย์สินที่แท้จริงหรือทรัพย์สินส่วนตัว หรือทรัพย์สินที่สามารถสืบเสาะได้ รวมถึงทรัพย์สินในการโอน

---

[68] United State Code; (Title 18 : Crimes and Criminal Procedure, Chapter 46 : Forfeiture , section 981). [online] Available from : http://caselaw.Ip.findlaw.com.

หรือการพยายามโอนเพื่อการกระทำความผิด ตามมาตรา 1956 หรือมาตรา 1957

1.2 ทรัพย์สินใดๆ ซึ่งเป็นทรัพย์สินที่แท้จริงหรือทรัพย์สินส่วนตัว ซึ่งหน่วยงานที่มีอำนาจหน้าที่ในการสืบเสาะทรัพย์สินที่ได้มาจากการกระทำใดๆอันเป็นการกระทำละเมิดต่อมาตรา 225, 656, 657,1005,1006,1007,1029,1030,1034 แห่งบทบัญญัติฉบับนี้ที่ได้กล่าวข้างต้น

1.3 ทรัพย์สินที่ได้มาจากการกระทำ การพยายาม หรือการสมรู้ร่วมคิดในการกระทำอันเป็น “ความผิดเฉพาะทางกฎหมาย” ตามที่ได้กำหนดไว้ในมาตรา 1956 (c) (7)

3. ผู้มีอำนาจในการริบทรัพย์สินดังกล่าวต้องกระทำโดยถือว่า ทรัพย์สินที่ต้องริบตามที่กำหนดข้างต้นเป็นทรัพย์สินที่ต้องริบแก่ประเทศสหรัฐอเมริกา ดังนั้นการริบทรัพย์สินดังกล่าวจึงต้องทำการยึดโดยผู้มีอำนาจแห่งรัฐ ซึ่งในที่นี้ หมายถึง อัยการสูงสุด หรือหากทรัพย์สินดังกล่าวอยู่ในอำนาจหน้าที่การสืบสวนสอบสวนของรัฐมนตรีว่าการกระทรวงการคลัง หรือตัวแทนจากสำนักงานการไปรษณีย์ เช่นนี้ กรณีดังกล่าวให้ผู้ที่มีอำนาจหน้าที่ดังกล่าวเป็นผู้ทำการยึดทรัพย์สินที่ต้องริบดังกล่าวแล้วแต่กรณี

4. การดำเนินการริบทรัพย์สินดังกล่าวให้ดำเนินการยึดตามเงื่อนไขแห่งกฎของรัฐบาลกลางว่าด้วยวิธีพิจารณาทางอาญา ข้อ 41 (Federal Rules of Criminal Procedure) ซึ่งกฎหมายกำหนดให้ โดยทั่วไปการยึดทรัพย์สินกำหนดให้ต้องมีหมายยึด และต้องได้รับอำนาจจากหมายค้นภายใต้กฎหมายฉบับนี้ ยกเว้นการยึดโดยปราศจากหมายค้น หากกรณี,

4.1 ผู้ร้องได้ยื่นคำร้องต่อศาลชั้นต้นแห่งเขตแห่งรัฐนั้นและศาลได้ออกหมายยึดทรัพย์สินดังกล่าว

4.2 มีเหตุอันสมควรในการริบทรัพย์สินนั้น และ

4.2.1 การยึดทรัพย์สินได้ดำเนินการตามกฎหมายว่าด้วยการจับหรือค้น

4.2.2 ข้อยกเว้นอย่างใดอย่างหนึ่งในการร้องขอออกหมาย

5. ทรัพย์สินต้องถูกยึดโดยชอบด้วยกฎหมายแห่งรัฐ หรือตัวแทนการบังคับใช้กฎหมายแห่งท้องถิ่นนั้นหรือตัวแทนของรัฐบาลกลาง

<u>กระบวนการริบทรัพย์สินภายใต้กฎของรัฐบาลกลางว่าด้วยวิธีพิจารณาทางอาญา ข้อ 41 (Federal Rules of Criminal Procedure)</u>

หากพิจารณาถึงกระบวนการริบทรัพย์สินภายใต้กฎของรัฐบาลกลางว่าด้วยวิธีพิจารณาทางอาญา ข้อ 41 (Federal Rules of Criminal Procedure) กำหนดให้ เจ้าพนักงานยุติธรรมแห่งศาลชั้นต้นที่มีเขตอำนาจแห่งรัฐที่ทรัพย์สินนั้นตั้งอยู่ หรือแห่งเขตอำนาจแห่งรัฐที่พบทรัพย์สินนั้นเป็นผู้ออกหมายยึดดังกล่าว หรือหากเป็นทรัพย์สินหรือบริการที่อยู่ในอำนาจแห่งรัฐต่างประเทศต้องมีการโอนอำนาจให้แก่พนักงานเจ้าหน้าที่ส่วนกลางแห่งรัฐบาลกลางของประเทศสหรัฐอเมริกาเป็นผู้มีอำนาจหน้าที่ในการดำเนินการดังกล่าวภายใต้พันธะกรณีแห่งสนธิสัญญาหรืออนุสัญญาระหว่างประเทศ ทั้งนี้ การโอนอำนาจในการยึดทรัพย์สินดังกล่าวจะต้องมีการฟ้องร้องต่อศาลชั้นต้นแห่งท้องถิ่นหรือศาลชั้นต้นแห่งรัฐนั้น เพื่อโอนอำนาจของรัฐบาลต่างประเทศดังกล่าวมาอยู่ในเขตอำนาจแห่งศาลชั้นต้นของท้องถิ่นหรือแห่งศาลชั้นต้นของรัฐ เพื่อการออกหมายยึดทรัพย์ดังกล่าว

ประกอบกับทรัพย์สินที่ริบภายใต้มาตรานี้จะไม่ถูกอายัดจนกว่าจะได้รับความเห็นจากอัยการสูงสุด หรือรัฐมนตรีว่าการกระทรวงการคลัง หรือตัวแทนผู้รับมอบอำนาจแห่งสำนักงานการไปรษณีย์แล้วแต่กรณี หรืออาจได้รับคำสั่งหรือคำพิพากษาจากศาลชั้นต้นที่มีเขตอำนาจดังกล่าว ซึ่งทรัพย์สินที่ถูกยึดตามมาตรานี้ผู้ที่มีอำนาจหน้าที่ดังกล่าวต้องเป็นผู้ประทับตราบนทรัพย์สินนั้น หรือเคลื่อนย้ายทรัพย์สินนั้นตามเห็นสมควร หรือเรียกร้องให้มีการเก็บรักษาที่เหมาะสมและถูกต้องตามกฎหมาย

นอกจากนั้น กรณีความผิดตามบทบัญญัติแห่งประมวลกฎหมายอาญานี้ซึ่งอยู่ภายใต้มาตรการการริบทรัพย์สินดังกล่าว แต่เกิดขึ้นในต่างประเทศถือว่าความผิดดังกล่าวอยู่ภายใต้เขตอำนาจแห่งประเทศสหรัฐอเมริกาได้โดยกรณี

1. หากบุคคลหนึ่งบุคคลใดถูกจับและถูกกล่าวหาในต่างประเทศในการกระทำความผิดข้างต้น บุคคลนั้นต้องถูกบังคับใช้มาตรการริบทรัพย์สินโดยประเทศสหรัฐอเมริกาภายใต้มาตรานี้ โดยผู้พิพากษา

แห่งรัฐบาลกลางหรือผู้พิพากษาแห่งศาลชั้นต้นเป็นผู้ออกคำสั่งในการริบทรัพย์สินดังกล่าวภายในระยะเวลาไม่เกิน สามสิบ วัน

2. โดยการฟ้องบุคคลชาวต่างประเทศดังกล่าวต้องอยู่ภายใต้เงื่อนไขว่าเหตุอันสมควรและเชื่อได้ว่าบุคคลดังกล่าวมีทรัพย์สินที่ต้องถูกยึดไว้โดยประเทศสหรัฐอเมริกาภายใต้มาตรานี้

3. ทรัพย์สินที่ถูกยึดตามมาตรานี้จะไม่มีคำสั่งคืนทรัพย์ หากได้มีการพิสูจน์ และลงความเห็นว่าเป็นทรัพย์สินที่อยู่ในอำนาจการยึดทรัพย์สินดังกล่าวของเจ้าพนักงานผู้มีอำนาจสืบสวนสอบสวนตามมาตรการริบทรัพย์สินนี้

อีกประการหนึ่ง หากทรัพย์สินที่ได้ยึดมาจากการกระทำความผิดดังกล่าวเป็นการทรัพย์สินที่ได้มาจากการกระทำความผิดต่อธนาคารหรือสถาบันทางการเงินแล้ว การยึดทรัพย์สินดังกล่าวต้องให้ตัวแทนหรือผู้มีอำนาจหน้าที่ของสถาบันทางการเงินต้องเป็นผู้ร่วมพิจารณาค่าชดเชยความเสียหายที่เกิดขึ้นแก่สถาบันทางการเงินจากการกระทำความผิดดังกล่าว

3.3.2 การริบทรัพย์สินทางอาญา

ประมวลกฎหมายอาญาแห่งสหรัฐอเมริกา ได้กำหนดถึง มาตรการริบทรัพย์สินทางอาญา ซึ่งถือเป็นมาตรการทางกฎหมายในการแก้ไขเยียวยาความเสียหายจากการกระทำอาชญากรรมที่เกิดขึ้น และมาตรการทางกฎหมายดังกล่าวได้ถูกบัญญัติไว้ให้ใช้บังคับกับการกระทำความผิดที่ได้บัญญัติไว้ในบทบัญญัติฉบับนี้เป็นการเฉพาะเช่นเดียวกับการริบทรัพย์สินทางแพ่ง ตามมาตรา 982 แห่งประมวลกฎหมายอาญานี้

มาตรา 982[69] ได้กำหนดถึงการริบทรัพย์สินทางอาญา เพื่อใช้บังคับการกระทำความผิดที่กำหนดไว้ในมาตรานี้โดยเฉพาะ และการริบทรัพย์สินดังกล่าวเป็นไปตามกระบวนการริบทรัพย์สินทางแพ่งตามมาตรา 981 โดยจะดำเนินการยึดทรัพย์สินตามจำนวนแห่งทรัพย์สินของผู้กระทำความผิด ไม่ว่าจะเป็นทรัพย์สินที่ได้มา ใช้ หรือที่เกี่ยวข้องกับการกระทำความผิดดังกล่าว โดยมีสาระสำคัญดังนี้

---

[69] United State Code, (Title 18 : Crimes and Criminal Procedure, Chapter 46 : Forfeiture , section 982) . [online] Available from : http://caselaw.lp.findlaw.com.

1. ความผิดที่ได้บัญญัติให้ใช้มาตรการริบทรัพย์สินทางอาญา และเป็นความผิดที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ตามที่กำหนดไว้ในมาตรา 982 ได้กำหนดให้เป็นความผิดลักษณะเดียวกับความผิดที่กำหนดให้ใช้มาตรการริบทรัพย์สินทางแพ่ง ดังที่ได้อธิบายแล้วข้างต้น

2. มาตรการริบทรัพย์สินทางอาญา จะใช้บังคับกับกรณีซึ่งศาลจะมีคำพิพากษาลงโทษบุคคลที่กระทำการ หรือบุคคลที่สมรู้ร่วมคิดในการกระทำการในความผิดที่กำหนดไว้ตามมาตรานี้และได้อธิบายแล้วข้างต้น โดยศาลจะมีคำสั่งริบทรัพย์สินใดๆ ซึ่งเป็นทรัพย์สินที่ประกอบ หรือได้รับมาจากการกระทำความผิด ไม่ว่าจะเป็นการได้รับทรัพย์สินนั้น โดยทางตรงหรือทางอ้อม ตามจำนวนของทรัพย์สินที่มีการละเมิดนั้นจริงแก่รัฐ

3.3.2 ประเทศสหราชอาณาจักร (United Kingdom)

หากพิจารณาถึงมาตรการในการริบทรัพย์สิน ซึ่งเกี่ยวข้องกับการกระทำความผิดและสร้างความเสียหายให้เกิดขึ้นจากกรณีดังกล่าว และจัดเป็นมาตรการสำคัญในการบังคับใช้กับความผิดร้ายแรง หรือจัดว่าเป็นความผิดหนักที่สร้างความเสียหายเป็นจำนวนมาก ซึ่งหากพิจารณามาตรการทางกฎหมายดังกล่าวแห่งประเทศสหราชอาณาจักรจะเห็นได้ว่า อาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในประเทศสหราชอาณาจักร ไม่ว่าจะเป็นความผิดตามความผิดที่เกี่ยวข้องกับการกระทำทางคอมพิวเตอร์ หรือความผิดต่อการฟอกเงินผ่านการโอนเงินทางอิเล็กทรอนิกส์นั้น ซึ่งในส่วนของความผิดที่เกี่ยวข้องกับการกระทำทางคอมพิวเตอร์และอยู่ในบังคับของพระราชบัญญัติการกระทำโดยมิชอบทางคอมพิวเตอร์ (Computer Misuse Act) มิได้กำหนดบทบัญญัติในการยึดหรือริบทรัพย์สินหรือเงินที่ได้จากการกระทำทางคอมพิวเตอร์นั้นแต่อย่างใด หากแต่บทบัญญัติดังกล่าวได้บัญญัติไว้เพียงมาตรการในการปรับโดยไม่จำกัดอัตราสูงสุดไว้เท่านั้น หรือการปรับตามดุลพินิจของศาลตามแต่เห็นสมควรในกรณีความผิดทางคอมพิวเตอร์ที่อาศัยโอกาส หรือความชำนาญในการกระทำความผิด

ส่วนความผิดกรณีการฟอกเงินผ่านการโอนเงินทางอิเล็กทรอนิกส์นั้น และประเทศสหราชอาณาจักรเป็นประเทศผู้นำหนึ่งในประเทศสมาชิกของสหภาพยุโรปและยึดถือหลัก

การในการดำเนินการต่างๆ ตามในการจัดการเงินที่ได้มาจากการกระทำความผิดเป็นไปตามอนุสัญญาว่าด้วยการค้น ยึด และริบทรัพย์สินเกี่ยวกับการฟอกเงินที่ได้จากการประกอบอาชญากรรม (Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime) ของสภาสหภาพยุโรป ซึ่งในปัจจุบันประเทศสหราชอาณาจักรได้มีบทบัญญัติทางกฎหมายในการจัดการกับเงินที่ได้มาหรือเงินที่เกี่ยวข้องกับการกระทำความผิดได้ตามพระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceed of Crime Act, 2002)

โดยหลักการสำคัญของการยึดเงินที่ได้มา หรือได้ประโยชน์หรือเกี่ยวข้องกับการกระทำความผิดเป็นกระบวนการหนึ่งที่สามารถหยุดกระบวนการโอนเงินโดยผิดกฎหมาย และหยุดยั้งโครงข่ายของอาชญากรรมดังกล่าวได้ รวมถึงสามารถช่วยหยุดยั้งกระบวนการสร้างความเสียหายทางการเงินการธนาคารได้[70]

พระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceed of Crime Act, 2002)

ตามพระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceed of Crime Act, 2002) ได้กำหนดบทบัญญัติ ในการจัดการยึดเงินที่ได้มา หรือได้ประโยชน์ หรือเกี่ยวข้องกับการกระทำความผิดไว้ในมาตรา 67[71] ซึ่งมีสาระสำคัญดังนี้

1. เงินดังกล่าวอาจเป็นเงินที่ได้มาจาก หรือได้ประโยชน์หรือเกี่ยวข้องกับการกระทำความผิด ซึ่งเป็นเงินที่ถือโดยบุคคล หรือเงินในบัญชีของธนาคารหรือสถาบันทางการเงิน
2. ให้อำนาจตำรวจ หรือเจ้าพนักงานศุลกากร เป็นผู้ยึดเงินดังกล่าวแล้วแต่กรณี โดย
   2.1 คำสั่งให้ระงับธุรกรรมต่างๆ เกี่ยวกับเงินนั้นทันที
   2.2 คำสั่งให้ยึดเงินที่บุคคลนั้นถืออยู่ในทันที

---

[70] Criminals 'cash To Be Seized Under New UK Powers. [online] Available from : http://www.Britain-info.org.

[71] The Proceed of Crime Act 2002, section 67. [online] Available from : http://www.Britain-info.org.

3. ศาลชั้นต้นจะเป็นผู้ออกคำสั่งริบเงินดังกล่าว หรือออกคำสั่งให้ธนาคาร หรือสถาบันทางการเงินจ่ายเงินดังกล่าวให้แก่รัฐ

จากบทบัญญัติข้างต้นจะเห็นได้ว่า การยึด ริบ เงินที่ได้มา ได้ประโยชน์ หรือเกี่ยวข้องกับการกระทำความผิดมีหลักการสำคัญอยู่ในมาตรา 67 แห่งพระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceed of Crime Act, 2002) แต่หากพิจารณาถึงหลักการสำคัญของการริบ เงินหรือทรัพย์สินที่ได้มา ได้ประโยชน์ หรือเกี่ยวข้องกับความผิดร้ายแรง (Serious Offence) ทั้งหมดมีสาระสำคัญ [72] ดังนี้

1. ให้อำนาจตำรวจหรือเจ้าพนักงานศุลกากรเป็นผู้ยึดเงินดังกล่าว โดยไม่มีจำกัดเขตอำนาจแห่งรัฐ หรือยึด ณ ที่ใดก็ได้ในประเทศสหราชอาณาจักร
2. ให้อำนาจเจ้าพนักงานในการค้นเงินที่ได้มา หรือเกี่ยวข้องกับการกระทำอาชญากรรม
3. ให้อำนาจเจ้าพนักงานในการยึดเงินดังกล่าวภายใน 48 ชั่วโมง หรือมากกว่านั้น นับแต่เจ้าพนักงานได้รับคำสั่งศาล
4. ให้อำนาจศาลเป็นผู้ออกคำสั่งริบ ซึ่งเป็นการยึดเงินที่ได้มา หรือเกี่ยวข้องกับการกระทำอาชญากรรม

3.3.3 สหภาพยุโรป (European Union)

หากพิจารณาถึง มาตรการทางกฎหมายในการกำหนดแก้ไขเยียวยาและหยุดยั้งความเสียหายที่เกิดขึ้นเกี่ยวกับอาชญากรรมที่เกิดขึ้นจากการฟอกเงิน ซึ่งรวมถึงการฟอกเงินผ่านการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งคณะกรรมาธิการแห่งสภาสหภาพยุโรปได้ร่วมกันวางแนวทางในการจัดการหรือดำเนินการกับอาชญากรรมร้ายแรง หรือมีผลกระทบต่อระบบเศรษฐกิจไว้ในอนุสัญญาว่าด้วยการค้น ยึดและริบทรัพย์สินเกี่ยวกับการฟอกเงินที่ได้จากการประกอบอาชญากรรม (Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime) เมื่อวันที่ 8 พฤศจิกายน 2533 (8 November 1990) ซึ่งมุ่งหมายให้เป็นการต่อต้านอาชญากรรมร้ายแรงและใช้ความก้าวหน้าทางด้านเทคโนโลยีที่มีอยู่ในปัจจุบันในการกระทำความผิด และกำลังเป็นปัญหาเพิ่มมากขึ้นในปัจจุบัน รวมถึงวางแนวนโยบายในการจัดการกับการฟอกเงินเพื่อเป็นการ

---

[72] Criminals 'cash To Be Seized Under New UK Powers. [online] Available from : http://www.Britain-info.org.

ปกป้องความมั่นคงของประเทศ ซึ่งอนุสัญญาดังกล่าวมีหลักการสำคัญเกี่ยวกับการจัดการกับอาชญากรรมร้ายแรงในการค้น ยึด ริบทรัพย์สิน โดยมีสาระสำคัญดังนี้

1. กำหนดแนวทางร่วมกันให้แก่นานาประเทศเกี่ยวกับมาตรการริบทรัพย์สิน

อนุสัญญาว่าด้วยการค้น ยึด และริบทรัพย์สินเกี่ยวกับการฟอกเงินที่ได้จากการประกอบอาชญากรรม (Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime) ได้กำหนดแนวทางร่วมกันเกี่ยวกับมาตรการริบทรัพย์สินให้แก่นานาประเทศไว้ในมาตรา 2 , มาตรา 3 และมาตรา 4 [73] ซึ่งมีหลักการสำคัญกล่าวคือ

1.1 กำหนดให้มาตรการในการยึดหรือริบทรัพย์สิน หรือสิ่งที่มูลค่าอย่างหนึ่งอย่างใดที่ได้มาจากผลประโยชน์ทางเศรษฐกิจ หรือเป็นผลต่อเนื่องมาจากการกระทำความผิดเป็นสิ่งจำเป็นในการยึดเครื่องมือหรืออุปกรณ์ในการประกอบอาชญากรรม ตามมาตรา 2

1.2 กำหนดให้มาตรการริบทรัพย์สินจำเป็นต้องอาศัยกระบวนการสืบสวนสอบสวนเป็นกรณีเฉพาะ โดยกำหนดกระบวนการสืบสวนสอบสวนพิเศษในการสืบเสาะทรัพย์สินที่ต้องบังคับใช้มาตรการริบทรัพย์สินตามมาตรา 2 ข้างต้น และมาตรการดังกล่าวต้องสามารถป้องกันการโอน หรือเปลี่ยนแปลงสถานะของทรัพย์สินนั้นได้ โดย

1.2.1 ให้อำนาจแก่ศาลหรือพนักงานเจ้าหน้าที่เชี่ยวชาญพิเศษสั่งตรวจความมีอยู่ของทรัพย์สินจากบันทึกของธนาคาร หรือสถาบันทางการเงินได้ โดยผู้มีอำนาจหน้าที่จะไม่เปิดเผยข้อมูลดังกล่าวตามเงื่อนไขพื้นฐานทางด้านความลับทางธนาคารตามมาตรา 3 และมาตรา 4

1.2.2 ให้อำนาจแก่พนักงานเจ้าหน้าที่เชี่ยวชาญพิเศษในการดักฟังการสื่อสารโทรคมนาคม การเข้าถึงระบบคอมพิวเตอร์ หรือขอเอกสารใดๆ เพื่อให้ความสะดวกในการสืบเสาะทรัพย์สินจากการประกอบ

---

[73] Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, article 2. [online] Available from : http://www.conventins.coe.int.

อาชญากรรมดังกล่าว รวมถึงรวบรวมพยานหลักฐานที่เกี่ยวข้อง ตามมาตรา 4 .

1.3 กำหนดให้การโอนทรัพย์สินที่ได้จากการกระทำความผิดหรืออาชญากรรมซึ่งถือเป็นความผิดตามกฎหมายภายในประเทศ เพื่อวัตถุประสงค์ในการปกปิดหรือปิดบังที่มาของทรัพย์สินนั้น หรือเพื่อสนับสนุนหรือมีส่วนร่วมในการกระทำความผิดถือเป็นความผิดฐานฟอกเงิน

2. มาตรการความร่วมมือระหว่างประเทศ

อนุสัญญาว่าด้วยการค้น ยึด และริบทรัพย์สินเกี่ยวกับการฟอกเงินที่ได้จากการประกอบอาชญากรรม (Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime) ได้กำหนดแนวทางซึ่งเป็นความร่วมมือระหว่างประเทศเกี่ยวกับกระบวนการในการริบทรัพย์สิน โดยมีหลักการและสาระสำคัญดังนี้

2.1 กำหนดให้ประเทศสมาชิกต้องกำหนดมาตรการในการให้ความช่วยเหลือในการสืบเสาะทรัพย์สินจากการประกอบอาชญากรรม ซึ่งความช่วยเหลือดังกล่าว รวมถึงการจัดให้มีมาตรการความปลอดภัยแก่พยานหลักฐานที่นำไปสู่การสืบเสาะถึงทรัพยสินที่ประกอบอาชญากรรม ตามมาตรา 8[74]

2.2 กำหนดให้ประเทศสมาชิกอาจทำการร้องขอให้ประเทศสมาชิกอื่นให้ทำการริบทรัพย์สินที่เกี่ยวข้อง หรือได้มาจากการประกอบอาชญากรรม กรณีทรัพย์สินนั้นอยู่ในเขตอำนาจแห่งรัฐประเทศสมาชิกดังกล่าว ตามมาตรา 13 [75]โดย

2.2.1 ทำการบังคับแห่งทรัพย์สินนั้น ภายใต้คำสั่งของศาลแห่งประเทศสมาชิกที่ร้องขอให้ทำการริบทรัพย์สินจากการประกอบอาชญากรรม

---

[74] Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, article 8. [online] Available from : http://www.conventins.coe.int.

[75] Ibid., article 13.

2.2.2 ยอมรับคำร้องขอของพนักงานเจ้าหน้าที่เชี่ยวชาญพิเศษที่ได้รับคำสั่งให้ริบทรัพย์สิน หรือได้รับอนุญาตในการบังคับการริบทรัพย์สินนั้น

2.2.3 ประเทศสมาชิกที่ได้รับคำร้องขอต้องทำการริบทรัพย์สินนั้น ภายใต้อำนาจแห่งกฎหมายภายในของตน

2.3 ทรัพย์สินที่ต้องถูกริบของประเทศที่ถูกร้องขอต้องเป็นทรัพย์สินที่ถูกกำหนดให้ริบได้ภายใต้กฎหมายภายในของประเทศที่ถูกร้องขอ และการร้องขอดังกล่าวไม่ตัดสิทธิในการริบทรัพย์สินดังกล่าวของตน ตามมาตรา 15 และมาตรา 16 [76]

3.4 มาตรการทางกฎหมายในการกำหนดหน่วยงานพิเศษเพื่อบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

มาตรการทางกฎหมายในการสืบสวนสอบสวนอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์เป็นมาตการที่กำหนดให้มีหน่วยงานเฉพาะที่มีความเชี่ยวชาญพิเศษเป็นหน่วยงานในการดำเนินการสืบสวน สอบสวน รวบรวมพยานหลักฐานต่างๆ ที่เกี่ยวข้องกับระบบการเงินการธนาคาร เพราะอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์นี้มีลักษณะเฉพาะหลายประการ ไม่ว่าจะเป็นระบบการเงินการธนาคารมีความซับซ้อนและเกี่ยวข้องโดยตรงกับระบบอิเล็กทรอนิกส์ หรือระบบคอมพิวเตอร์ ดังนั้นการดำเนินการสืบสวนสอบสวน รวมรวมพยานหลักฐาน หรือแม้แต่การดำเนินกระบวนวิธีพิจารณาในการริบทรัพย์สินที่ได้มา หรือเกี่ยวข้องกับอาชญากรรมดังกล่าวจึงต้องมีลักษณะพิเศษและอาศัยความรู้ ความเชี่ยวชาญเฉพาะ ด้วยเหตุนี้ กฎหมายที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์จึงมีการกำหนดหน่วยงานพิเศษในการสืบสวนสอบสวน หรือดำเนินการบังคับใช้กฎหมายกับอาชญากรรมดังกล่าว

[76] Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, article 15 and 16. [online] Available from : http://www.conventins.coe.int.

3.4.1 ประเทศสหรัฐอเมริกา (United State)

ประเทศสหรัฐอเมริกาได้กำหนดหน่วยงานพิเศษที่มีอำนาจหน้าที่ในการดำเนินการสืบสวนสอบสวนคดีที่มีลักษณะความผิดเฉพาะ ตามประมวลกฎหมายอาญา (Federal Crime and Criminal Procedure) ที่ได้กำหนดลักษณะความผิดต่างๆ ที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ และบางลักษณะความผิดซึ่งถือเป็นความผิดเฉพาะ ดังนั้น ประมวลกฎหมายอาญาจึงได้มีการกำหนดหน่วยงานพิเศษที่มีอำนาจหน้าที่ในการบังคับใช้กฎหมายกับกรณีดังกล่าวโดยเฉพาะ ไม่ว่าจะเป็นความผิดต่อการแสดงอุปกรณ์อิเล็กทรอนิกส์ปลอมหรือให้ข้อมูลทางอิเล็กทรอนิกส์อันเป็นเท็จเพื่อฉ้อโกงการโอนเงินทางอิเล็กทรอนิกส์ทางธนาคารตามมาตรา 514 หรือความผิดต่อการเข้าถึงบัตร รหัส หรือสื่ออิเล็กทรอนิกส์ ตามมาตรา 1029 หรือความผิดต่อการเข้าถึงเครื่องคอมพิวเตอร์โดยปราศจากอำนาจตามมาตรา 1030 นั้น ประมวลกฎหมายอาญาได้กำหนดให้ **THE UNITED STATE SECRET SERVICE (USSS)** เป็นหน่วยงานพิเศษที่มีอำนาจหน้าที่ในการทำการสืบสวนสอบสวนความผิดดังกล่าว

นอกจากนั้น ความผิดต่อการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งได้กำหนดไว้ในประมวลกฎหมายอาญามาตรา 1956 และมาตรา 1957 นั้น ความผิดดังกล่าวได้มีหน่วยงานที่รับผิดชอบอยู่ 3 หน่วยงาน กล่าวคือ หน่วยงานแรก **THE FINANCIAL CRIMES ENFORCEMENT NETWORK (FinCEN)** เป็นหน่วยงานพิเศษสังกัดกระทรวงการคลัง มีอำนาจหน้าที่ตามพระราชบัญญัติต่อต้านการฟอกเงินระหว่างประเทศและการก่อการร้าย ค.ศ. 2001 (International Money Laundering Abatement Act : IMLA) ที่กำหนดไว้ในพระราชบัญญัติว่าด้วยต่อต้านการก่อการร้าย (USA Patriot Act) มาตรา 361 และ หน่วยงานที่สอง **Money Laundering Section** สังกัดกระทรวงยุติธรรมมีอำนาจหน้าที่ตามพระราชบัญญัติควบคุมการฟอกเงิน Money Laundering Act ตามประมวลกฎหมายอาญา และหน่วยงานที่สาม **The Office of the Financial Enforcement** สังกัดกระทรวงการคลังมีอำนาจหน้าที่ตามพระราชบัญญัติความลับทางธนาคาร

3.4.1.1 THE UNITED STATE SECRET SERVICE (USSS)

U.S.S.S หรือ The Secret Service เป็นหน่วยงานพิเศษที่ได้เริ่มจัดตั้งขึ้นเมื่อวันที่ 5 กรกฎาคม ค.ศ. 1850 ณ กรุงวอชิงตัน ดี.ซี. และมีอำนาจหน้าที่พิเศษในการสืบสวนสอบสวนคดีทางเศรษฐกิจหรือทางการเงินการธนาคาร โดยกองสืบสวนสอบสวนอาชญากรรมทางการธนาคาร (Financial Crimes Division : FCD) เป็นหน่วยงานหลักภายใต้ U.S.S.S ในการ

ทำหน้าที่สืบสวนสอบสวนคดีทางการเงินการธนาคาร ไม่ว่าจะเป็นการวางแผน การตรวจสอบการสืบสวนสอบสวนอาชญากรรมต่อระบบการธนาคาร ซึ่งรวมถึงการฉ้อโกงธนาคาร (bank fraud) การฉ้อโกงเข้าถึงทางอิเล็กทรอนิกส์ (access device) การฉ้อโกงคอมพิวเตอร์ (Computer Fraud) ไม่ว่าจะเป็นระบบการชำระเงินอัตโนมัติ เครื่องรับฝากถอนเงินอัตโนมัติ หรือการฝากเงินทางธนาคาร รวมถึงการโอนเงินทางอิเล็กทรอนิกส์ด้วย (Electronic Fund Transfer : EFT)

ซึ่งเมื่อวันที่ 5 พฤศจิกายน ค.ศ. 1990 ประเทศสหรัฐอเมริกาได้มีการจัดตราบทบัญญัติในการกำหนดเขตอำนาจแก่ The Secret Service ให้มีอำนาจในการสืบสวนสอบสวนความผิดเกี่ยวกับการฉ้อโกงหรือการกระทำอันเป็นการต่อต้านความมั่นคงปลอดภัยทางธนาคารหรือสถาบันทางการเงิน เช่นเดียวกับอำนาจในการสืบสวนสอบสวนความผิดลักษณะต่างๆ ของหน่วยงานของกระทรวงยุติธรรม และในปัจจุบัน The Secret Service มีอำนาจหน้าที่หลักดังนี้[77]

1. มีขอบเขตอำนาจในการสืบสวนสอบสวนเช่นเดียวกับหน่วยงานสืบสวนสอบสวนของกระทรวงยุติธรรม
2. ติดตั้งโปรแกรมการตรวจสอบการฉ้อโกงธนาคาร (Financial Institution Fraud : FIF Program) โดยโปรแกรมดังกล่าวจะถูกออกแบบให้ทำหน้าที่ในการจัดการตรวจสอบการเดินทางบัญชีเพื่อป้องกันอาชญากรรมที่เกิดขึ้น
3. สนับสนุนโครงการความร่วมมือระหว่างประเทศในการต่อต้านอาชญากรรมรูปแบบใหม่ๆ ทางการธนาคาร
4. การให้ความร่วมมือในการให้ข้อมูลแก่องค์กรธนาคารแห่งอเมริกัน (American Banking Association) เกี่ยวกับอาชญากรรมที่เกิดขึ้นทางการเงินการธนาคารที่เพิ่มสูงขึ้น
5. ดำเนินการสืบสวนสอบสวนคดีทางการเงินการธนาคาร ไม่ว่าจะเป็นการฉ้อโกงบัตรเครดิต หรืออุปกรณ์อิเล็กทรอนิกส์ที่อำนวยความสะดวก หรือการสร้างข้อมูลเฉพาะในการใช้เทคโนโลยีคอมพิวเตอร์ ซึ่งมีรายละเอียดดังนี้

---

[77] Financial Crimes Division. Financial Institution Fraud (FIF) and Related Criminal Investigations.[online] Available from : http//www. secretservice.gov.

5.1 การแสดงอุปกรณ์อิเล็กทรอนิกส์ปลอมหรือให้ข้อมูลทางอิเล็กทรอนิกส์อันเป็นเท็จเพื่อฉ้อโกงการโอนเงินทางอิเล็กทรอนิกส์ทางธนาคารตามมาตรา 514 ซึ่งได้ตราขึ้นในปี 1996 เพื่อบังคับใช้กับความผิดต่อการฉ้อโกงอุปกรณ์อิเล็กทรอนิกส์ที่ให้อำนวยความสะดวกต่อการให้บริการทางธนาคารดังกล่าว

5.2 การฉ้อโกงต่อการเข้าถึงอุปกรณ์ทางอิเล็กทรอนิกส์ ตามมาตรา 1029 ไม่ว่าจะเป็นการเข้าถึงบัตรเดบิต บัตรเอทีเอ็ม รหัสทางคอมพิวเตอร์ รหัสข้อมูลเฉพาะบุคคล (PINs)

5.3 การฉ้อโกงคอมพิวเตอร์ ตามมาตรา 1030

6. จัดให้มีความช่วยเหลือหรือสนับสนุนหน่วยงานที่มีอำนาจในการยึดหรือริบทรัพย์สินจากการกระทำความผิดข้างต้น ไม่ว่าจะเป็นการให้คำปรึกษา หรือความรู้ความชำนาญในการสืบเสาะทรัพย์สินที่ต้องยึดหรือริบดังกล่าว

7. อำนาจหน้าที่ในการยึดและเก็บรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ ซึ่งเป็นองค์ประกอบสำคัญในการบังคับใช้กฎหมายในการดำเนินคดีกับความผิดลักษณะดังกล่าว ซึ่งหน่วยงานดังกล่าวได้มีการกำหนด หลักปฏิบัติที่ดีที่สุดในการเก็บรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ (Best Practices for Seizing Electronic Evidence) ซึ่งหลักดังกล่าวจะมีการกำหนดลักษณะพิเศษของอุปกรณ์อิเล็กทรอนิกส์หรือคอมพิวเตอร์ไว้ เพื่อพัฒนาและให้ความรู้แก่พนักงานเจ้าหน้าที่ของหน่วยงานดังกล่าวให้มีความเข้าใจพื้นฐานเกี่ยวกับอุปกรณ์หรือเครื่องคอมพิวเตอร์นั้นๆ

3.4.1.2 The Financial Crimes Enforcement Network (FinCEN)

FinCEN ถือเป็นหน่วยงานพิเศษที่สังกัดกระทรวงการคลัง ซึ่งจัดตั้งขึ้นเมื่อ 25 เมษายน ค.ศ. 1990 โดยมีอำนาจหน้าที่ในการสืบเสาะข้อมูลทางการเงินจากหลายหน่วยงาน และนำข้อมูลดังกล่าวมาวิเคราะห์เพื่อนำไปใช้ประโยชน์ให้แก่หน่วยงานที่เกี่ยวข้อง ประกอบกับการฟอกเงินทางธนาคารเป็นกระบวนการหลักที่ง่ายและสะดวกที่สุด ดังนั้นการสืบเสาะข้อมูล

ดังกล่าวจึงรวมถึงการสืบเสาะข้อมูลทางการเงินการธนาคารด้วย ซึ่งจัดได้ว่าหน่วยงานนี้ถือเป็นศูนย์ข้อมูลทางการเงินในด้านต่างๆ โดยข้อมูลดังกล่าวจะนำมาใช้ประโยชน์และเป็นมาตรการเบื้องต้นในการป้องกันการฟอกเงินภายในประเทศและการฟอกเงินระหว่างประเทศ ซึ่งหากพิจารณาถึง วัตถุประสงค์ในการจัดตั้งหน่วยงานดังกล่าวจะเห็นได้ว่า โดยหน่วยงานดังกล่าวจะมีอำนาจหน้าที่ซึ่งสรุปได้ดังนี้

1. การสนับสนุนหน่วยงานผู้ปฏิบัติหน้าที่หรือหน่วยงานผู้มีหน้าที่สืบสวนสอบสวนโดยตรงในกรณีการฟอกเงิน
2. สนับสนุนการดำเนินการยึดหรือริบทรัพย์สินที่ได้มาจากการฟอกเงิน
3. นำข้อมูลทางการเงินที่เกี่ยวข้องไปใช้ประโยชน์ในการกำหนดนโยบายระดับประเทศ

3.4.1.3 Money Laundering Section

หน่วยงานนี้ถือเป็นหน่วยงานพิเศษที่สังกัดกระทรวงยุติธรรม Criminal Division มีอำนาจหน้าที่โดยตรงในการสืบสวนสอบสวนกรณีการฟอกเงิน ตามพระราชบัญญัติควบคุมการฟอกเงิน (Money Laundering Act) แห่งประมวลกฎหมายอาญา โดยหน่วยงานดังกล่าวจะมีอำนาจหน้าที่ซึ่งสรุปได้ดังนี้

1. ดำเนินการติดตามรายการทางบัญชีที่เกี่ยวข้องหรือต้องสงสัยอย่างใกล้ชิด
2. ดำเนินมาตรการในการริบทรัพย์สินทางแพ่ง และมาตรการในการริบทรัพย์สินทางอาญาตามมาตรา 981 และมาตรา 982 แห่งประมวลกฎหมายอาญา
3. ให้ความสำคัญและให้ความร่วมมือในระดับระหว่างประเทศในการดำเนินการริบและแบ่งปันทรัพย์สินที่เกี่ยวข้อง รวมทั้งประสานงานกับหน่วยงานที่มีอำนาจหน้าที่เช่นเดียวกันในทางต่างประเทศ

3.4.1.4 The Office of Financial Enforcement

หน่วยงานนี้ถือเป็นหน่วยงานพิเศษซึ่งสังกัดกระทรวงการคลังเช่นเดียวกับ FinCEN โดยจัดตั้งขึ้นเมื่อค.ศ. 1970 ตามพระราชบัญญัติความลับทางธนาคาร (Bank Secrecy Act) ซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับธนาคารหรือสถาบันทางการเงินเกี่ยวกับรายการทางบัญชีต่างๆ

ตามพระราชบัญญัติความลับทางธนาคารดังกล่าว โดยหน่วยงานดังกล่าวจะมีอำนาจหน้าที่ซึ่งสรุปได้ดังนี้

1. อำนาจหน้าที่ในการบังคับใช้กฎหมายเกี่ยวกับรายการทางบัญชีทางธนาคารให้ต้องปฏิบัติตามพระราชบัญญัติความลับทางธนาคาร
2. จัดเก็บข้อมูลทางการเงินหรือทางบัญชีของธนาคารหรือสถาบันทางการเงิน
3. อำนาจหน้าที่ในการสืบสวนการกระทำความผิดตามพระราชบัญญัติความลับทางธนาคาร

3.4.2 ประเทศสหราชอาณาจักร (United Kingdom)

ประเทศสหราชอาณาจักรได้กำหนดให้ **FSA** หรือ **Financial Service Authority** เป็นหน่วยงานพิเศษที่มีอำนาจหน้าที่ในการดำเนินการสืบสวนสอบสวนคดีที่มีลักษณะความผิดเฉพาะหรือคดีซึ่งเป็นความผิดทางการเงินการธนาคารไว้โดยเฉพาะ FSA ถือว่ามีอำนาจหน้าที่ในการสืบสวนสอบสวนคดีทางการเงินการธนาคารอย่างสมบูรณ์ ตามพระราชบัญญัติการให้บริการทางการธนาคารค.ศ. 2001 (The Financial Services and Markets Act) โดยมีวัตถุประสงค์หลักในการให้อาชญากรรมที่เกิดขึ้นทางการธนาคารลดน้อยลง หรือวางมาตรการที่เหมาะสมเกี่ยวกับอาชญากรรมที่เกิดขึ้น ไม่ว่าจะเป็น อาชญากรรมซึ่งกระทำการอันโดยมิชอบทางการธนาคาร การฉ้อโกงหรือการกระทำทุจริตทางการธนาคาร รวมถึงการฟอกเงินทางการธนาคาร โดยหน่วยงานดังกล่าวจะมีอำนาจหน้าที่ซึ่งสรุปได้ดังนี้

1. การสร้างโปรแกรมการตรวจสอบความล้มเหลวเกี่ยวกับข้อมูลเฉพาะของบุคคลที่เกี่ยวกับธุรกรรมทางการเงินการธนาคารในการฟอกเงินผ่านทางธนาคาร
2. การพัฒนาแนวทางในการวางมาตรการในการบังคับใช้กฎหมายกับการฟอกเงินทางธนาคารให้เป็นไปตามมาตรการระดับระหว่างประเทศ
3. การสร้างมาตรฐานของระบบธนาคารในการต่อต้านการฟอกเงิน
4. การให้ความร่วมมือการพนักงานเจ้าหน้าที่ในกระบวนยุติธรรมทางอาญาในการบังคับใช้กฎหมายกับการฟอกเงิน
5. การเก็บบันทึกข้อมูลทางการเงินที่เพียงพอต่อการสืบสวนสอบสวนการกระทำความผิด
6. การวิเคราะห์ข้อมูลทางการเงินเพื่อการควบคุมการฟอกเงินทางการธนาคาร

ทั้งนี้จะเห็นได้ว่า FSA มิใช่หน่วยงานพิเศษในการสืบสวนสอบสวนอาชญากรรมที่เกิดขึ้นในระบบการเงินการธนาคาร โดย FSA มิได้มีอำนาจหน้าที่ในการสืบสวนสอบสวนหรือดำเนินมาตรการในการค้น ยึด หรือริบทรัพย์สิน หากแต่ FSA เป็นหน่วยงานพิเศษที่มีอำนาจหน้าที่ในการสนับสนุน ช่วยเหลือในการสืบสวน สวบสวนหรือการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมที่เกิดขึ้นต่อระบบทางการเงินการธนาคารให้เป็นไปอย่างมีประสิทธิภาพ

ตามพระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceeds of Crime Act, 2002) ได้มีการจัดตั้ง ARA หรือ Assets Recovery Agency ให้เป็นหน่วยงานพิเศษในการดำเนินมาตรการสนับสนุนการค้น ยึด หรือสืบเสาะทรัพย์สินที่เกี่ยวกับการกระทำความผิดฐานฟอกเงิน เพื่ออำนวยความสะดวกแก่พนักงานเจ้าหน้าที่หรือเพื่อให้เป็นไปตามพระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 ได้อย่างมีประสิทธิภาพ [78] กล่าวคือ

1. ช่วยเหลือในการสืบเสาะทรัพย์สินที่เกี่ยวกับความผิดฐานฟอกเงิน
2. สนับสนุนมาตรการในการสืบสวนสอบสวนความผิดฐานฟอกเงิน
3. สนับสนุนมาตรการค้น ยึดของพนักงานเจ้าหน้าที่ที่มีอำนาจหน้าที่ตามคำสั่งของศาลชั้นต้น

[78] Explanatory Notes to Proceeds of Crime Act, 2002. [online] Available from : http://www.legal500.com.

ทั้งนี้จะเห็นได้ว่า FSA มิใช่หน่วยงานพิเศษในการสืบสวนสอบสวนอาชญากรรมที่เกิดขึ้นในระบบการเงินการธนาคาร โดย FSA มิได้มีอำนาจหน้าที่ในการสืบสวนสอบสวนหรือดำเนินมาตรการในการค้น ยึด หรือริบทรัพย์สิน หากแต่ FSA เป็นหน่วยงานพิเศษที่มีอำนาจหน้าที่ในการสนับสนุน ช่วยเหลือในการสืบสวน สวบสวนหรือการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมที่เกิดขึ้นต่อระบบทางการเงินการธนาคารให้เป็นไปอย่างมีประสิทธิภาพ

นอกจากนั้น ตามพระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceeds of Crime Act, 2002) ได้มีการจัดตั้ง ARA หรือ Assets Recovery Agency ให้เป็นหน่วยงานพิเศษอีกหน่วยงานหนึ่งในการดำเนินมาตรการสนับสนุนการค้น ยึด หรือริบทรัพย์สินที่เกี่ยวกับการกระทำความผิดฐานฟอกเงิน เพื่ออำนวยความสะดวกแก่พนักงานเจ้าหน้าที่หรือผู้ที่มีอำนาจในการค้น ยึด หรือริบทรัพย์สิน เพื่อให้เป็นไปตามพระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 ได้อย่างมีประสิทธิภาพ [78] กล่าวคือ

1. ช่วยเหลือในการสืบเสาะทรัพย์สินที่เกี่ยวกับความผิดฐานฟอกเงิน
2. สนับสนุนมาตรการในการสืบสวนสอบสวนความผิดฐานฟอกเงิน
3. สนับสนุนมาตรการค้น ยึดของพนักงานเจ้าหน้าที่ที่มีอำนาจหน้าที่ตามคำสั่งของศาลชั้นต้น

3.5 มาตรการทางกฎหมายว่าด้วยความร่วมมือระหว่างประเทศ

3.5.1 ธนาคารกลางระหว่างประเทศ (Banking for International Settlement)

Bank For International Settlements (BIS) เป็นองค์กรความร่วมมือประเทศทางด้านการเงินการธนาคารระหว่างประเทศที่เก่าแก่ที่สุดของโลก ซึ่งตั้งอยู่ ณ ประเทศสวิสเซอร์แลนด์ โดยองค์กรดังกล่าวมีหน้าที่หลักในการสนับสนุน กำกับดูแลและวางมาตรการทางการเงินการธนาคารให้เป็นมาตรฐานแก่ระบบการเงินการธนาคาร และธนาคารกลางของแต่ละประเทศทั่วโลก ซึ่งมาตรฐานของ Bank For International Settlements (BIS) นี้ถือว่าได้รับการยอมรับโดยทั่วไปว่ามาตรฐานดังกล่าวเป็นมาตรฐานสากล โดย Bank For International Settlements (BIS) ได้วางมาตรฐานอันเป็นหลักปฏิบัติในการให้บริการทางด้านการเงินการธนาคารระหว่างประเทศ รวมถึงการโอนเงินทางอิเล็กทรอนิกส์ เพื่อเป็นการควบคุมการให้บริการทางด้านการเงินการธนาคารของ

---

[78] Explanatory Notes to Proceeds of Crime Act, 2002. [online] Available from : http://www.legal500.com.

แต่ละประเทศต่างๆ ให้เหมาะสม สร้างความน่าเชื่อถือและลดความเสี่ยงที่อาจเกิดขึ้นแก่การให้บริการทางด้านการเงินการธนาคาร และสามารถรองรับสถานะของกฎหมายที่พัฒนาและเปลี่ยนแปลงไปในปัจจุบัน

ด้วยเหตุนี้ หลักปฏิบัติในการโอนเงินทางอิเล็กทรอนิกส์ของ Bank For International Settlements (BIS) หรือที่เรียกว่า ข้อกำหนดของบาเซิลซึ่งได้กำหนดให้การโอนเงินทางอิเล็กทรอนิกส์ต้องอยู่ภายใต้หลักปฏิบัติอันเหมาะสมต่อลูกค้า (Customer Due Diligence) ไว้ใน Basel Committee on Banking Supervision- Customer due diligence for Bank ซึ่งมีสาระสำคัญสรุปได้ดังนี้

1. การให้ลูกค้าแสดงตนที่แท้จริง
2. สถาบันทางการเงิน หรือธนาคารต้องปฏิบัติตามหลักปฏิบัติอันเหมาะสมต่อลูกค้า หรือ Customer Due Diligence โดยหลักดังกล่าวกำหนดให้สถาบันทางการเงินต้องให้บริการภายใต้มาตรฐาน KYC (Know Your Customer) เพราะเหตุว่าสถาบันการเงินหรือธนาคารต้องรู้ข้อมูลเฉพาะหรือตัวตนที่แท้จริงของลูกค้า
3. การปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่ใช้บังคับในเรื่องการโอนเงิน หรือ ประเพณีปฏิบัติทางบัญชี
4. การให้ลูกค้าเปิดเผยข้อมูลทางบัญชี
5. การให้ความร่วมมือกับเจ้าหน้าที่ตามกฎหมาย โดยให้ข้อมูลของลูกค้าเท่าที่จะให้ได้

อย่างไรก็ตาม ข้อกำหนดดังกล่าวยังมีจุดบกพร่องหรือปัญหาในการใช้บังคับอยู่หลายประการ กล่าวคือ

1. ข้อกำหนดดังกล่าวได้วางมาตรฐานการให้บริการ หรือหลักปฏิบัติที่เหมาะสมของการให้บริการ แต่มิได้วางบทบัญญัติหรือมาตรฐานการรองรับกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นอาชญากรรมที่กระทำต่อระบบอิเล็กทรอนิกส์หรือระบบคอมพิวเตอร์เพื่อให้ได้มาซึ่งการโอนเงิน หรืออาชญากรรมที่อาศัยการโอนเงินเป็นเครื่องมือในการกระทำความผิด ซึ่งหากพิจารณาถึงการกระทำความผิดโดยอาชญากรที่มีความรู้ความสามารถทางด้านคอมพิวเตอร์ และอาศัยความชำนาญทางด้านระบบการโอนเงินดังกล่าว และกระทำการอันเป็นความผิดข้างต้นแล้วจะสามารถบังคับใช้กับกรณีดังกล่าวได้อย่างไร

2. ข้อกำหนดดังกล่าวไม่มีผลผูกพันตามกฎหมาย และเป็นเพียงข้อกำหนดในทางระหว่างประเทศ ซึ่งผลการใช้บังคับของข้อกำหนดดังกล่าวต้องอาศัยความร่วมมือระหว่างประเทศเป็นองค์ประกอบสำคัญ
3. พนักงานเจ้าหน้าที่ที่มีอำนาจหน้าที่ทางการเงินการธนาคารจะสามารถสังเกตพฤติกรรมการโอนเงินเพื่อกระทำความผิดได้อย่างไร ซึ่งการโอนเงินทางอิเล็กทรอนิกส์โดยทั่วไปเป็นวิธีการการดำเนินธุรกิจโดยปกติเท่านั้น
4. การส่งข้อมูลของการโอนเงินทางอิเล็กทรอนิกส์ เพื่อการปฏิบัติงานหรือตรวจสอบของพนักงานเจ้าหน้าที่ หรือผู้ที่เกี่ยวข้องกับการป้องกันและปราบปรามการฟอกเงินอาจทำได้ไม่มากนักเพราะการโอนเงินทางอิเล็กทรอนิกส์ในปัจจุบันมีจำนวนมาก
5. หน่วยงานที่มีหน้าที่เฉพาะในการตรวจสอบ ติดตาม สืบสวน สอบสวน หรือรวบรวมพยานหลักฐานที่เกี่ยวกับอาชญากรรมดังกล่าวจะต้องมีความรู้ความชำนาญทางด้านคอมพิวเตอร์และระบบการเงินการธนาคาร รวมถึงกระบวนการรับส่งข้อมูลทางอิเล็กทรอนิกส์ของระบบการเงินการธนาคารจึงจะสามารถทำหน้าที่ดังกล่าวได้อย่างมีประสิทธิภาพ

นอกจากจุดบกพร่องของข้อกำหนดดังกล่าวแล้ว กรณีการบังคับใช้มาตรการความร่วมมือระหว่างประเทศดังกล่าวยังมีปัญหาและอุปสรรคสำคัญของมาตรการดังกล่าวใน 2 กรณี[79] กล่าวคือ

1. มาตรการตรวจสอบลูกค้าธนาคาร

มาตรการในการตรวจสอบลูกค้าธนาคาร ตามหลักปฏิบัติของธนาคารหรือสถาบันทางการเงินยังมีประเด็นปัญหาที่เกิดขึ้นได้ ดังต่อไปนี้

1.1 ผู้ทำการโอนเงินซึ่งเป็นนิติบุคคล จะสามารถตรวจสอบความถูกต้องของเจ้าของนิติบุคคลนั้นได้อย่างไร เพราะบางกรณีผู้ถือหุ้น กรรมการ หรือกรรมการผู้จัดการนั้นอาจไม่ใช่เจ้าของที่แท้จริงของนิติบุคคลดังกล่าว

---

[79] ปาริชาต มุสิกะปาน, “มาตรการในการป้องกันและปราบปรามการฟอกเงิน : ศึกษากรณีเทคโนโลยีสารสนเทศในเครือข่ายอินเตอร์เน็ทกับการฟอกเงิน” (วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชานิติศาตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย,2543), หน้า 112.

1.2 ที่มาของเงินทุนของนิติบุคคลไม่มีที่มาที่เจ้าหน้าที่ตรวจสอบได้

1.3 ธนาคารหรือสถาบันทางการเงินไม่อาจมีข้อมูลของลูกค้า หรือนิติบุคคลที่เกี่ยวข้องกับกระบวนการฟอกเงินได้

1.4 กรณีฟอกเงินโดยพนักงาน หรือผู้บริหารของธนาคาร หรือสถาบันทางการเงินยิ่งทำให้มีความซับซ้อนในการเข้าไปติดตามสืบสวนสอบสวนกรณีดังกล่าว

2. มาตรการในการรายงานการโอนเงินทางอิเล็กทรอนิกส์

หากพิจารณาถึง มาตรการในการรายงานการโอนเงินทางอิเล็กทรอนิกส์ยังคงมีช่องว่างในการบังคับใช้กฎหมายกับการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าว กล่าวคือ

2.1 การรายงานการโอนเงินทางอิเล็กทรอนิกส์ของลูกค้าหรือผู้โอนนั้นจะแสดงถึงที่มาของเงินจำนวนดังกล่าวได้อย่างไร ซึ่งโดยทั่วไปการรายงานการโอนเงินทางอิเล็กทรอนิกส์นั้นจะต้องรายงานเฉพาะกรณีเฉพาะที่น่าสงสัย

2.2 ในกรณีการฟอกเงินโดยความร่วมมือของผู้บริหารสถาบันทางการเงินหรือธนาคารพาณิชย์นั้นยิ่งเป็นการกระทำที่ยากต่อการตรวจสอบและไม่เหลือร่องรอยใดๆ ดังนั้นการควบคุมภายในของสถาบันการเงินหรือธนาคารพาณิชย์ จึงต้องอาศัยความชำนาญเฉพาะหรือจิตใต้สำนึกของการเดินบัญชีอย่างปกติในการควบคุมภายในของสถาบันทางการเงินหรือการธนาคาร

3.5.2 โครงการความร่วมมือระหว่างประเทศในการต่อต้านการฟอกเงินทางการเงินการธนาคาร (Financial Action Task Force: FATF)

FATF เป็นโครงการความร่วมมือระหว่างประเทศ เพื่อต่อต้านการฟอกเงินทางการเงินการธนาคารผ่านสถาบันการเงินต่าง ๆ โดย FATF เกิดจากการความร่วมมือระหว่างประเทศในการประชุมสุดยอดทางเศรษฐกิจของกลุ่มประเทศอุตสาหกรรม 7 ประเทศ หรือกลุ่ม G 7 เมื่อเดือนกรกฎาคม ค.ศ.1989 โดยที่ประชุมได้มีมติจัดตั้งคณะทำงานเฉพาะกิจเพื่อแก้ไขปัญหาของการฟอกเงินโดยเฉพาะมีชื่อเรียกว่า Financial Action Task Force (FATF) และ FATF ได้ประกาศรายงานของตนอย่างเป็นทางการเมื่อเดือนเมษายน ค.ศ. 1990 ซึ่งปัจจุบัน FATF มีสมาชิกทั้งหมด 26 ประเทศ ประกอบด้วย ประเทศกลุ่ม OECD ทั้ง 24 ประเทศได้แก่

ออสเตรเลีย เบลเยี่ยม แคนาดา เดนมาร์ก ฝรั่งเศส เยอรมัน กรีซ ไอซ์แลนด์ อิตาลี ลักเซมเบริก์ เนเธอร์แลนด์ นอร์เวย์ โปรตุเกส สเปน สวีเดน สวิตเซอร์แลนด์ ตุรกี สหราชอาณาจักร สหรัฐอเมริกา ญี่ปุ่น ออสเตรีย ฟินแลนด์ นิวซีแลนด์ สิงค์โปร์ และ ฮ่องกง[80]

FATF ได้มีความร่วมมือร่วมกันในระดับประเทศในการร่วมกันพิจารณาและวางแนวทางร่วมกันในการต่อต้านการฟอกเงินทางการเงินการธนาคาร ซึ่งได้กำหนดไว้ในข้อแนะนำ 40 ประการของโครงการความร่วมมือระหว่างประเทศในการฟอกเงินทางการเงินการธนาคาร หรือ FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING รวมถึงแนวทางในการต่อต้านการก่อการร้ายทางการเงินการธนาคาร ซึ่งได้กำหนดไว้ในข้อแนะนำพิเศษในการต่อต้านการก่อการร้ายทางการเงินการธนาคาร (FATF Special Recommendations on Terrorist Financing) ซึ่งมีแต่ละโครงการดังกล่าวมีแนวทางและข้อแนะนำในการวางมาตรการทางด้านกฎหมายให้แก่ประเทศต่างๆ ซึ่งจะได้อธิบายรายละเอียดต่อไป

<u>ข้อแนะนำ 40 ประการ ของโครงการความร่วมมือระหว่างประเทศในการฟอกเงินทางการเงินการธนาคาร (FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING)</u>

ข้อแนะนำ 40 ประการของโครงการความร่วมมือระหว่างประเทศในการฟอกเงินทางการเงินการธนาคาร (FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING)[81] นั้น มีสาระสำคัญดังนี้

1. ประเทศสมาชิกแต่ละประเทศ ควรกระทำการให้สัตยาบันและปฏิบัติตามข้อสัญญาเวียนนา ค.ศ. 1988 โดยทันที
2. ควรมีการปรับปรุงกฎหมายเรื่องการเปิดเผยความลับของสถาบันการเงินเพื่อไม่ให้เป็นอุปสรรคต่อการนำข้อแนะนำดังกล่าวมาปฏิบัติ

---

[80] ปาริชาต มุสิกะปาน. “มาตรการในการป้องกันและปราบปรามการฟอกเงิน : ศึกษากรณีเทคโนโลยีสารสนเทศในเครือข่ายอินเตอร์เนตกับการฟอกเงิน”. (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต ภาคนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย), 2543.

[81] Financial Action Task Force on Money Laundering. “Report” (Paris, February 6th , 1990)

3. ควรกำหนดมาตรการต่อต้านการฟอกเงินผิดกฎหมาย รวมถึงการเพิ่มความร่วมมือและข้อกฎหมายโดยรวมที่ช่วยสนับสนุนการสืบสวน การดำเนินการตามกฎหมาย และการส่งผู้ร้ายข้ามแดน
4. ประเทศสมาชิกแต่ละประเทศควรมีปฏิบัติตามมาตรการต่างๆ และมาตรการทางกฎหมายในการต่อต้านการฟอกเงินที่ได้จากการค้ายาเสพติดที่เป็นความผิดทางอาญา
5. ประเทศสมาชิกควรกำหนดมาตรการทางกฎหมายในการเพิ่มบทลงโทษสำหรับการฟอกเงินที่ได้รับมาจากการค้ายาเสพติดให้หนักเท่ากับโทษของอาชญากรรมร้ายแรงประเภทอื่นๆ
6. ควรกำหนดมาตรการทางกฎหมายในการบังคับใช้กับกรณีความผิดจากการฟอกเงินอย่างน้อยตั้งแต่เริ่มล่วงรู้ถึงการทำธุรกรรมทางการเงินที่เข้าข่ายการฟอกเงินดังกล่าว เพราะการรับรู้ดังกล่าวแสดงให้เห็นถึงเจตนารมย์ในการบังคับใช้กฎหมายอย่างหนึ่ง
7. ธนาคาร สถาบันทางการเงิน หรือพนักงานเจ้าหน้าที่ทางธนาคารหรือพนักงานเจ้าหน้าที่ของสถาบันทางการเงินที่ทำการฟอกเงินโดยผิดกฎหมายควรมีความผิดทางอาญาร่วมกัน
8. ประเทศต่างๆ ควรจะจัดให้มีมาตรการต่างๆ เท่าที่จำเป็นตามข้อสัญญาเวียนนากำหนด ซึ่งรวมถึงมาตรการด้านกฎหมายเพื่อให้เจ้าหน้าที่ผู้รักษากฎหมายสามารถยึดหรืออายัดทรัพย์สินใดๆ ที่ได้มา หรือเป็นเครื่องมือของการฟอกเงินผิดกฎหมาย และมาตรการทางกฎหมายในการกำหนดบทลงโทษทั้งทางอาญา ทางแพ่ง และทางการเงิน
9. ข้อแนะนำที่ 12-29 ในข้อแนะนำ 40 ประการนี้ควรมีผลบังคับใช้กับธนาคารและสถาบันทางการเงินอื่นๆ ด้วย
10. ประเทศต่างๆ ควรมีการดำเนินการเพื่อให้องค์การต่างๆ ที่มีการทำธุรกิจเกี่ยวข้องกับการชำระเงินสดจำนวนมากๆ ต้องปฏิบัติตามข้อแนะนำ 40 ประการนี้ให้มากที่สุดเท่าที่ทำได้
11. ควรจะกำหนดประเภทของสถาบันทางการเงินที่ใช่ธนาคารและสถาบันทางการอื่นๆ ที่ทำธุรกิจเกี่ยวข้องกับเงินสด ต้องปฏิบัติตามข้อแนะนำ 40 ประการนี้ให้สอดคล้องกันในแต่ละประเทศ
12. ธนาคารหรือสถาบันทางการเงินไม่ควรมีบัญชีซึ่งปกปิดชื่อจริงของลูกค้า หรือใช้ชื่อบัญชีปลอม และควรมีกฎหมาย กฎเกณฑ์ ข้อกำหนด หรือข้อตกลงระหว่างธนาคารและสถาบันทางการเงินว่า ต้องให้ลูกค้าแสดงตนพร้อม

หลักฐานของตน (Identifying Document) และต้องบันทึกประวัติไว้ เมื่อเริ่มทำธุรกิจหรือดำเนินธุรกรรมให้ลูกค้า

13. ธนาคารหรือสถาบันทางการเงินควรมีมาตรการที่จะได้มาซึ่งข้อมูลประวัติที่แท้จริงของลูกค้าโดยเฉพาะในกรณีที่มีผู้อื่นากระทำการแทนให้
14. สถาบันทางการเงินควรเก็บประวัติการทำธุรกรรมต่างๆ ไว้อย่างน้อย 5 ปี ทั้งนี้ เพื่อให้สามารถให้ข้อมูลแก่ผู้รักษากฎหมายได้ในกรณีที่ถูกร้องขอ เพื่อประกอบการสืบสวนหรือดำเนินคดี
15. สถาบันทางการเงินควรจะให้ความสนใจกับธุรกรรมที่มีมูลค่าสูง หรือธุรกรรมที่มีรูปแบบผิดไปจากธรรมดา เช่น การกระทำที่ไม่มีเหตุผลในทางเศรษฐกิจและทางกฎหมาย และควรสืบหาข้อเท็จจริง ความเป็นมา และวัตถุประสงค์ในการทำธุรกรรมทางการเงินนั้น เพื่อให้มีข้อมูลที่สามารถช่วยงานของผู้ตรวจสอบหรือผู้รักษากฎหมายในความผิดฐานฟอกเงิน
16. ควรมีกฎหมายในการคุ้มครองธนาคารหรือสถาบันทางการเงิน และเจ้าหน้าที่ของสถาบันทางการเงิน เพื่อไม่ให้มีความผิดในฐานะที่เปิดเผยข้อมูลที่เกี่ยวข้องกับธุรกรรมที่สงสัยว่าจะเกี่ยวข้องกับอาชญากรรมให้แก่เจ้าหน้าที่ผู้รักษากฎหมาย
17. สถาบันทางการเงิน ผู้บริหาร และเจ้าหน้าที่ของสถาบันทางการเงินไม่ควรจะแจ้งให้ลูกค้าทราบถึงการรายงานแก่เจ้าหน้าที่ผู้รักษากฎหมายเกี่ยวกับข้อมูลที่เกี่ยวข้องกับลูกค้า
18. สถาบันทางการเงินต้องรายงานถึงธุรกรรมที่น่าสงสัย ตามข้อแนะนำของเจ้าหน้าที่ผู้รักษากฎหมาย
19. ประเทศที่ไม่มีข้อกำหนดให้ธนาคารหรือสถาบันทางการเงินรายงานธุรกรรมทางการเงินที่น่าสงสัยของลูกค้า และลูกค้าไม่รายงานข้อมูลเกี่ยวกับการทำธุรกรรมทางการเงินซึ่งสถาบันทางการเงินควรปฏิเสธที่จะให้ความช่วยเหลือหรือมีความสัมพันธ์กับลูกค้า และปิดบัญชีของลูกค้านั้น
20. ธนาคารหรือสถาบันทางการเงินควรจัดให้มีโครงการต่อต้านการฟอกเงิน ซึ่งอย่างน้อยประกอบด้วยการกำหนดนโยบาย กรรมวิธี และการควบคุมภายในองค์กร การแต่งตั้งให้เจ้าหน้าที่ระดับบริหารดูแลให้เป็นไปตามนโยบายดังกล่าว ตลอดจนการจัดให้มีการคัดเลือกพนักงานที่มีคุณภาพ จัดให้มีการฝึกอบรมพนักงานและให้มีกลไกตรวจสอบระบบการต่อต้านการฟอกเงินโดยผิดกฎหมาย

21. ธนาคารหรือสถาบันทางการเงินควรจะให้ความสนใจ และเพ่งเล็งความสัมพันธ์ทางธุรกิจและการทำธุรกรรมกับบุคคล หรือนิติบุคคลของประเทศที่ไม่ได้นำข้อแนะนำ 40 ประการนี้ไปบังคับใช้ โดยเฉพาะในกรณีที่ธุรกรรมทางการเงินนั้นไม่มีเหตุผลทางเศรษฐกิจและกฎหมาย ซึ่งธนาคารหรือสถาบันทางการเงินควรจะกำหนดให้สอบและบันทึกประวัติบุคคลดังกล่าวไว้ก่อน
22. ธนาคารหรือสถาบันทางการเงินควรจะให้สาขาหรือบริษัทย่อยของตนในสาขาต่างประเทศปฏิบัติตามหลักเกณฑ์ที่กล่างข้างต้นให้มากที่สุดเท่าที่กฎหมายของประเทศที่ตั้งสำนักงานนั้นๆ จะอนุญาตให้ทำได้ สำหรับกรณีที่กฎหมายของประเทศที่สำนักงานตั้งอยู่ไม่อนุญาตให้ปฏิบัติตามหลักเกณฑ์ดังกล่าวได้ให้สถาบันทางการเงินแจ้งให้เจ้าหน้าที่ผู้รักษากฎหมายในประเทศที่สถาบันแม่ตั้งอยู่ทราบด้วย
23. ควรจะได้มีการศึกษาถึงความเป็นไปได้ ที่จะดำเนินมาตรการสืบสวนและกำกับการควบคุมการขนส่งเงินสดข้ามแดนอย่างเข้มงวดโดยไม่เป็นอุปสรรคต่อการเคลื่อนย้ายเงินทุนโดยเสรี
24. ประเทศต่างๆ ควรจะพิจารณาถึงความเป็นไปได้และประโยชน์ของการกำหนดให้สถาบันทางการเงินและตัวกลางต่างๆ ต้องรายงานธุรกรรมทางการเงินตราทั้งภายในประเทศและระหว่างประเทศที่มีมูลค่าสูงและเป็นไปตามที่กำหนดไว้ของหน่วยงานกลางทางการ ซึ่งหน่วยงานดังกล่าวจะทำหน้าที่รวบรวมข้อมูลในคอมพิวเตอร์ เพื่อเป็นประโยชน์ต่อพนักงานเจ้าหน้าที่ผู้รักษากฎหมายที่มีอำนาจหน้าที่ในการดำเนินคดีกรณีการฟอกเงิน
25. ประเทศต่างๆ ควรมีมาตรการในการสนับสนุน พัฒนาการทางด้านเทคนิคการบริหารเงินใหม่ ๆ เพื่อทดแทนการโอนเงินเปลี่ยนมือ เช่น การใช้เช็ค การให้บัตรอิเล็กทรอนิกส์ หรือการนำเงินฝากเข้าบัญชีโดยตรง
26. เจ้าหน้าที่ผู้ควบคุมดูแล และกำกับการดำเนินงานสถาบันทางการเงินหรือตัวกลาง หรือผู้รักษากฎหมายอื่นๆ ควรจะดำเนินการให้สถาบันที่อยู่ภายในการกำกับของตนมีมาตรการป้องกันการฟอกเงินผิดกฎหมายอย่างเพียงพอ และเจ้าหน้าที่เหล่านี้ควรจะให้ความร่วมมือกันระหว่างประเทศเพื่อการสืบสวนและดำเนินคดีการฟอกเงินผิดกฎหมาย
27. เจ้าหน้าที่ผู้รักษากฎหมาย ควรจะกำกับและออกกฎหมายเพื่อควบคุมกิจการที่ใช้เงินสดในการดำเนินธุรกิจ และกำหนดให้กิจการนั้นต้องปฏิบัติตามข้อแนะนำ 40 ประการนี้

28. เจ้าหน้าที่ผู้รักษากฎหมาย หรือเจ้าหน้าที่ผู้ควบคุมดูแล และกำกับการดำเนินงานสถาบันทางการเงินหรือตัวกลาง ควรกำหนดแนวทางในการช่วยให้สถาบันทางการเงินตรวจพบพฤติกรรมที่น่าสงสัยของลูกค้า และควรจะได้มีการปรับปรุงและพัฒนาแนวทางนี้อยู่เสมอ
29. เจ้าหน้าที่ผู้รักษากฎหมาย หรือเจ้าหน้าที่ผู้ควบคุมดูแล และกำกับการดำเนินงานสถาบันทางการเงินหรือตัวกลาง ควรจะใช้มาตรการทางกฎหมายที่จำเป็นเพื่อป้องกันอาชญากรรมหรือผู้สมรู้ร่วมคิดที่เข้าครอบงำกิจการของธนาคารหรือสถาบันทางการเงิน
30. ควรจะให้มีบันทึกรายการเงินสดหมุนเวียนระหว่างประเทศเพื่อจะได้สามารถประมาณการ ปริมาณเงินสดที่หมุนเวียนกับประเทศต่างๆ ได้
31. เจ้าหน้าที่ผู้รักษากฎหมายระหว่างประเทศควรจะรับผิดชอบในการรวบรวมและเผยแพร่ข้อมูลให้แก่เจ้าหน้าที่ผู้รักษากฎหมายอื่นๆ ทราบถึงเรื่องการฟอกเงินผิดกฎหมายล่าสุดและเทคนิคต่างๆ ที่เกิดขึ้นดังกล่าวพร้อมๆ กับให้ธนาคารกลางและผู้กำกับ ควบคุมดูแลธนาคารก็ควรที่จะดำเนินการรวบรวมและเผยแพร่ข้อมูลดังกล่าวเช่นเดียวกันผ่านเครือข่ายของตน
32. ประเทศต่างๆ ควรจะดำเนินการเพื่อสนับสนุนการแลกเปลี่ยนข้อมูลเกี่ยวกับธุรกรรมที่น่าสงสัย ตามที่เจ้าหน้าที่ผู้รักษากฎหมายของประเทศอื่นๆ ร้องขอ ทั้งนี้ควรจะมีการปกป้องให้การแลกเปลี่ยนข้อมูลดังกล่าวนี้เป็นไปอย่างสอดคล้องกับข้อกำหนดภายในประเทศและระหว่างประเทศในเรื่องการคุ้มครองสิทธิส่วนบุคคล (Privacy) และการคุ้มครองข้อมูลส่วนบุคคล (Data protection)
33. ประเทศต่างๆ ควรจะดำเนินการเพื่อให้แน่ใจว่าความแตกต่างของมาตรฐานความรู้ด้านคำจำกัดความเรื่องการกระทำความผิดโดยการฟอกเงินผิดกฎหมายของนานาประเทศเป็นไปในแนวทางเดียวกัน และไม่เป็นอุปสรรคต่อความสามารถหรือความตั้งใจของนานาประเทศในการให้ความช่วยเหลือหรือร่วมมือกันทางด้านกฎหมายร่วมกัน (Mutual Legal Assistance)
34. การร่วมมือระหว่างประเทศควรจะได้รับการสนับสนุนจากข้อตกลงและการดำเนินการในระดับประเทศ และความร่วมมือระหว่างประเทศซึ่งมีหลักการทางกฎหมายร่วมกันในอันที่จะมีมาตรการที่จะให้มีการช่วยเหลือกันและกันมากที่สุด

35. ประเทศต่างๆ ควรจะสนับสนุนให้มีสัญญาในทางระหว่างประเทศ เช่น อนุสัญญาของ สภาสหภาพยุโรปในเรื่องการอายัดทรัพย์สินที่ได้มาจากการกระทำความผิดทางกฎหมาย เป็นต้น
36. ควรสนับสนุนให้เจ้าหน้าที่ผู้รักษากฎหมายของประเทศต่างๆ ร่วมมือกันในการสืบสวน
37. ควรมีมาตรการในการช่วยเหลือระหว่างประเทศเกี่ยวกับมาตรการทางกฎหมายในการบังคับใช้ในเรื่องต่างๆ เช่นการจัดให้สถาบันทางการเงินหรือบุคคลอื่นๆ ที่เกี่ยวข้องจัดทำบันทึกรายงานการค้นหาบุค คลและหลักฐานต่างๆ ในการสืบสวนสอบสวน และดำเนินคดีในต่างประเทศ
38. ควรจัดให้มีเจ้าหน้าที่ดำเนินการเร่งด่วนเพื่อสนองตอบตามที่ต่างประเทศร้องขอในการชี้ตัว ยึดและอายัดทรัพย์สินจากการฟอกเงิน
39. เพื่อเป็นการป้องกันการขัดแย้งในเรื่องของเขตอำนาจศาล ในกรณีคดีที่อยู่ภายใต้การดำเนินคดีของหลายประเทศจึงต้องมีการพิจารณาเครื่องมือ และกลไกในการพิจารณาคดีที่เหมาะสมที่สุด สำหรับการดำเนินคดีกับผู้ต้องหาอย่างยุติธรรมและทำนองเดียวกันต้องมีการดำเนินการความร่วมมือในการยึดและอายัดทรัพย์สินซึ่งรวมถึงการแบ่งจัดสรรทรัพย์ที่ยึดมาได้ระหว่างกัน
40. ประเทศต่างๆ ควรมีกรรมวิธีในการส่งตัวผู้ต้องหาข้ามแดน ในกรณีการฟอกเงินโดยการโอนเงินระหว่างประเทศ

ซึ่งหากพิจารณาถึงข้อเสนอแนะ 40 ประการของ FATF ข้างต้นนั้นมีหลักการที่เป็นการต่อต้านการใช้ระบบธนาคารเพื่อการฟอกเงินของประเทศสมาชิก FATF โดยข้อเสนอแนะดังกล่าวมีหลักการสอดคล้องกับหลักการในการต่อต้านการฟอกเงินแห่งอนุสัญญาสหประชาชาติว่าด้วยการลักลอบค้ายาเสพติดและวัตถุออกฤทธิ์ต่อจิตประสาท ค.ศ. 1988 (หรืออนุสัญญาเวียนนา 1988) โดยมีหลักการสำคัญสรุปได้ดังนี้[82]

[82] Financial Action Task Force on Money Laundering, “Annual Report 2000-2001” (Paris, February 21 June, 2001), p.17.

1. มาตรการในการป้องกันและปราบปรามการฟอกเงินทางการเงินการธนาคาร

ข้อเสนอแนะดังกล่าวได้กำหนดกฎหมายว่าด้วยการเปิดเผยความลับของธนาคาร (Bank Secrecy Act) และข้อกำหนดเรื่องรายงานธุรกรรมทางการธนาคารให้เป็นไปตามหลักการต่อไปนี้

1.1 การแสดงตนของลูกค้า

โดยลูกค้าหรือผู้ใช้บริการทางธนาคารหรือสถาบันทางการเงินจะต้องเปิดเผยข้อมูลที่แท้จริงของตน และประเทศสมาชิกของ FATF ทุกประเทศจะไม่อนุญาตให้มีการใช้ชื่อบัญชีที่ปกปิดชื่อจริงของลูกค้า (Anonymous Accout) ทั้งมีข้อกำหนดให้ลูกค้าต้องทำการแสดงตนในการฝากเงินด้วย

1.2 การเก็บประวัติข้อมูลของลูกค้าในการทำธุรกิจ

ซึ่ง ประเทศสมาชิก FATF บางประเทศกำหนดให้ธนาคารหรือสถาบันทางการเงินต้องทำการเก็บประวัติข้อมูลของลูกค้าในการทำธุรกิจไว้ โดยมีจุดมุ่งหมายเพื่อการต่อต้านการฟอกเงินที่ได้มาโดยผิดกฎหมายและอาชญากรรมอื่น ๆ ทั้งนี้ ข้อมูลของลูกค้าในการเก็บประวัติดังกล่าว ได้แก่ ข้อมูลด้านธุรกิจ เงินสดมูลค่าสูงสุดหรือข้อมูลธุรกิจด้านต่างประเทศเป็นต้น ข้อมูลเหล่านี้จะถูกส่งมอบให้ผู้รักษากฎหมานไว้ในกรณีมีคำสั่งของศาล

1.3 การสืบค้นหาธุรกิจที่ต้องสงสัย

การสืบค้นหาธุรกิจที่น่าสงสัยในระบบการเงินของประเทศสมาชิก FATF สามารถกระทำได้โดยอาศัยวิธีการให้ธนาคารหรือสถาบันทางการเงินจัดตั้งระบบตรวจค้นหาธุรกิจที่น่าสงสัยนั้นต่อเจ้าหน้าที่ผู้รักษากฎหมายได้โดยไม่มีความรับผิดในข้อหาเปิดเผยความลับของลูกค้า แต่ทั้งนี้ธนาคารของประเทศสมาชิก FATF บางประเทศก็ยังไม่สามารถรายงานธุรกิจดังกล่าวได้เพราะเป็นการขัดต่อกฎหมาย Secrecy Law ในขณะที่บางประเทศ เช่น สหรัฐอเมริกา การไม่รายงานธุรกิจดังกล่าวถือเป็นความผิด

2. การกำหนดมาตรการในการลงโทษการฟอกเงินทางการธนาคาร

ข้อกำหนดของ FATF กำหนดให้ประเทศสมาชิกต้องมีบทบัญญัติหรือมาตรการทางกฎหมายในการลงโทษการฟอกเงินที่ได้มาจากการกระทำความผิดต่อกฎหมายลักษณะต่างๆ ที่แตกต่างกันไป ด้วยเหตุว่าบางประเทศกำหนดลักษณะของการกระทำความผิดเฉพาะการกระทำโดยเจตนา หรือบางประเทศกำหนดลักษณะของการกระทำความผิดที่เป็นการละเลยหรือเพิกเฉยโดยมิได้มีเจตนาดังกล่าว ดังนั้นจึงควรมีมาตรการทางกฎหมายในการกำหนดบทลงโทษในแต่ละลักษณะความผิดให้ครอบคลุมทุกกรณี ทั้งนี้บทลงโทษดังกล่าวรวมถึงการปรับ การจำคุก และการห้ามไม่ให้ประกอบอาชีพบางประเภทที่เกี่ยวข้องกับการกระทำความผิด

3. กำหนดมาตรการทางกฎหมายในการแก้ไขเยียวยาความเสียหายที่เกิดขึ้นจากการกระทำความผิดดังกล่าว

โดยส่วนใหญ่ประเทศสมาชิกของ FATF จะมีมาตรการภายในประเทศเกี่ยวกับมาตรการในการริบทรัพย์สิน กล่าวคือ การยึด และอายัดทรัพย์สินเฉพาะทรัพย์สินที่ได้มาจากการค้ายาเสพติด แต่ก็มีบางประเทศเท่านั้นที่มาตรการทางกฎหมายในการบังคับใช้มาตรการในการริบทรัพย์สินครอบคลุมไปถึงการริบทรัพย์สินที่เกี่ยวข้องกับการฟอกเงินโดยผิดกฎหมาย แต่เพื่อให้สามารถหยุดยั้งความเสียหายอันเกิดจากอาชญากรรมร้ายแรงต่างๆ และนำเอาระบบการเงินการธนาคารมาเป็นเครื่องมือในการกระทำความผิด ประเทศต่างๆ จึงควรปฏิบัติตามข้อเสนอแนะดังกล่าว

4. มาตรการในการกำหนดนโยบายทางการเงินการธนาคารแก่ธนาคารหรือสถาบันทางการเงินการธนาคารเกี่ยวกับกรณีความผิดการฟอกเงินผ่านธนาคารหรือสถาบันทางการเงิน

โดยข้อเสนอแนะดังกล่าวได้กำหนดนโยบายในการปฏิบัติมาตรการควบคุมการฟอกเงิน เพื่อให้เป็นแนวทางแก่ธนาคาร สถาบันทางการเงิน เจ้าหน้าที่ผู้รักษากฎหมาย หน่วยงานกลางที่เกี่ยวข้องต้องยึดถือและปฏิบัติตาม ตามที่ข้อกำหนดที่ได้กำหนดไว้ในข้อเสนอแนะ 40 ประการข้างต้น

ข้อแนะนำพิเศษในการต่อต้านการก่อการร้ายทางการธนาคาร (FATF Special Recommendations on Terrorist Financing)

FATF ได้มีการออกข้อแนะนำพิเศษในการต่อต้านการก่อการร้ายทางการธนาคาร (FATF Special Recommendation on Terrorist Financing) [83] ซึ่งมีรายละเอียดสรุปได้ดังนี้

1. ประเทศต่างๆ ควรมีการวางมาตรการให้ธนาคาร หรือสถาบันทางการเงินต้องเก็บรวบรวมข้อมูลที่ถูกต้องทั้งหมด ไม่ว่าจะเป็นข้อมูลเกี่ยวกับ ชื่อ ที่อยู่ และหมายเลขบัญชีที่เกี่ยวกับการโอนเงินหรือกระทำธุรกรรมทางการเงินการธนาคารต่างๆ ทั้งข้อมูลของผู้โอน ผู้ที่ได้รับโอน หรือผู้ที่เกี่ยวข้องที่อยู่ในโครงข่ายของการโอนเงินดังกล่าวทั้งหมด

2. ประเทศต่างๆ ควรมีการวางมาตรการเช่นเดียวกับมาตรการการต่อต้านการฟอกเงินเพื่อบังคับใช้กับการกระทำอันเป็นการก่อการร้ายทางการเงินการธนาคารที่สร้างความเสียหายให้แก่ระบบการเงินการธนาคาร

3. ประเทศต่างๆ ควรมีการวางมาตรการในการหยุดหรือระงับการโอนเงินหรือทรัพย์สินอื่นๆ ที่เกี่ยวข้องกับการก่อการร้ายทางการเงินการธนาคารโดยทันที และควรมีการวางมาตรการในการยึดหรือริบเงินหรือทรัพย์สินที่ใช้ หรือถูกใช้ หรือได้มาจากการก่อการร้ายทางการเงินการธนาคาร

4. ธนาคารหรือสถาบันทางการเงินต้องมีการรายงานการกระทำความผิดดังกล่าวไม่ว่าจะเป็นการฟอกเงินหรือการก่อการร้ายทางการเงินการธนาคารให้แก่ธนาคารหรือสถาบันทางการเงินอื่นๆ ที่ให้บริการเช่นเดียวกันได้ทราบข้อมูลดังกล่าว

5. ประเทศต่างๆ ควรจัดให้มีมาตรการทางกฎหมายในการสนับสนุนความให้ช่วยเหลือ หรือให้มีความเชื่อมโยงระหว่างกันในการบังคับใช้กฎหมายทั้งทางแพ่ง ทางอาญา หรือในการสืบสวนสอบสวนกรณีดังกล่าว

---

[83] Financial Special Recommendations on Terrorist Financing , 31 October, 2001.

บทที่ 4

ข้อพิจารณาเกี่ยวกับการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ในต่างประเทศเพื่อบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

เนื่องจากอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์เป็นอาชญากรรมที่จัดว่ามีความซับซ้อน และอาศัยเทคโนโลยีทางคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์อันทันสมัยในการกระทำความผิด ด้วยเหตุว่า อาชญากรรมดังกล่าวเป็นอาชญากรรมที่เกิดขึ้นภายใต้ระบบการโอนเงินทางอิเล็กทรอนิกส์ของระบบการเงินการธนาคาร ดังนั้นพยานหลักฐานที่เกิดขึ้นจึงย่อมมีความแตกต่างจากพยานหลักฐาน ไม่ว่าจะเป็น พยานวัตถุ หรือพยานเอกสารโดยทั่วไป ประกอบกับมาตรการทางกฎหมายในการบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์จำเป็นที่จะต้องอาศัยพยานหลักฐานทางคอมพิวเตอร์หรือพยานหลักฐานทางอิเล็กทรอนิกส์ ซึ่งเป็นพยานหลักฐานที่ได้มาจากคอมพิวเตอร์เป็นเครื่องมือสำคัญในการพิสูจน์ถึงการกระทำอันเป็นความผิดดังกล่าว

ซึ่งข้อพิจารณาสำคัญในการบังคับใช้กฎหมายกับความผิดลักษณะดังกล่าว กล่าวคือ หากมาตรการทางกฎหมายในการบังคับใช้กับอาชญากรรมที่เกิดขึ้นครบถ้วนสมบูรณ์ แต่หากขาดมาตรการทางกฎหมายทางด้านพยานหลักฐานในการบังคับใช้กับอาชญากรรมดังกล่าวแล้ว กรณีดังกล่าวก็ไม่อาจนำมาตรการทางกฎหมายมาบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพ

4.1 ข้อพิจารณาทางด้านการรับฟังพยานหลักฐานทางคอมพิวเตอร์ของประเทศสหรัฐอเมริกา

ตามกฎหมายลักษณะพยานแห่งประเทศสหรัฐอเมริกา (Federal Rules of Evidence Act) ได้กำหนดหลักเกณฑ์ในการรับฟังพยานหลักฐานทางคอมพิวเตอร์ หรือพยานหลักฐานทางอิเล็กทรอนิกส์ไว้ ซึ่งการรับฟังพยานหลักฐานดังกล่าวมีข้อพิจารณาหลายประการ ดังรายละเอียดสรุปได้ดังนี้

4.1.1 การรับฟังพยานหลักฐานตามหลักการรับฟังพยานหลักฐานที่ดีที่สุด

กฎหมายลักษณะพยานของประเทศสหรัฐอเมริกา (Federal Rules of Evidence Act) ได้ยึดถือตาม **“หลักการรับฟังพยานหลักฐานที่ดีที่สุด (Best Evidence Rule)”** เป็น

พยานหลักฐานที่สามารถรับฟังได้ ด้วยเหตุนี้ กฎหมายลักษณะพยาน (Federal Rule of Evidence Act) จึงได้มีการแก้ไขเพิ่มเติมบทบัญญัติเกี่ยวกับการรับฟังพยานหลักฐานทางคอมพิวเตอร์ พยานหลักฐานทางอิเล็กทรอนิกส์ ไว้ในมาตรา 1001[1] โดยกำหนดให้

(1) "เอกสารหรือบันทึก" อันหมายถึง อักษร ข้อความ ตัวเลขหรือสิ่งเทียบเท่าอย่างหนึ่งอย่างใด ซึ่งที่ถูกทำขึ้นโดยการเขียน พิมพ์ดีด เครื่องพิมพ์ การถ่ายสำเนา การถ่ายรูป การกระทำโดยการกระตุ้นแม่เหล็ก การบักทึกโดยเครื่องมือจักรกล เครื่องอิเล็กทรอนิกส์ หรือการประมวลผลข้อมูล

(2) "ภาพถ่าย" หมายรวมถึง ภาพนิ่ง, ฟิล์มเอกซเรย์, วีดิทัศน์ และภาพยนตร์

(3) "ต้นฉบับ" หมายถึง ต้นฉบับของข้อเขียนหรือบันทึก ซึ่งก็คือตัวข้อเขียนหรือบันทึกนั้นเอง หรือคู่ฉบับใดๆ ซึ่งผู้ทำหรือผู้ออกมีเจตนาให้เป็นผลเช่นนั้น ต้นฉบับของรูปถ่ายรวมตลอดถึงฟิล์มหรือรูปที่อัดได้นั้น ถ้ามีข้อมูลถูกเก็บบันทึกไว้ในคอมพิวเตอร์หรือเครื่องอื่นๆ โดยข้อมูลจากคอมพิวเตอร์ดังกล่าวต้องสามารถอ่านได้โดยสายตา หรือซึ่งแสดงได้ว่าข้อมูลดังกล่าวเป็นข้อมูลที่ถูกต้องและนับว่าเป็นต้นฉบับ

(4) คู่ฉบับ หมายถึง สิ่งที่ถูกผลิตขึ้น โดยให้มีผลเช่นเดียวกับต้นฉบับจากแม่พิมพ์ ภาพถ่าย หรือการถูกผลิตขึ้นโดยจากการประมวลผลของเครื่องคอมพิวเตอร์ หรือเครื่องบันทึกอิเล็กทรอนิกส์ หรือกระบวนการผลิตทางเคมีหรือกระบวนการผลิตขึ้นโดยทางเทคนิคอย่างอื่น โดยให้มีผลที่ถูกต้องเช่นเดียวกับต้นฉบับ

จากการศึกษาจากมาตราดังกล่าว จะเห็นได้ว่า บทบัญญัติดังกล่าวได้มีบัญญัติให้มีการยอมรับฟังถึงพยานหลักฐานดังต่อไปนี้

1. การรับฟังข้อมูลจากเครื่องคอมพิวเตอร์ หรือถูกทำขึ้น จากเครื่องพิมพ์แรงกระตุ้นแม่เหล็กไฟฟ้า หรือเครื่องอิเล็กทรอนิกส์ ตามมาตรา 1001 (1)
2. การยอมรับเอกสารจากคอมพิวเตอร์ (Printout) ซึ่งจัดเป็นข้อมูลที่ได้ถูกเก็บบันทึกไว้ในเครื่องคอมพิวเตอร์ ตามมาตรา 1003 (3) ซึ่งประเด็นนี้รวมถึงการยอมรับข้อมูลจาก แผ่นดิสก์ (Disk) ซึ่งจัดได้ว่าเป็น "ต้นฉบับ" ตามมาตรา 1003 ซึ่งเป็นข้อมูลที่ถูกบันทึกจากคอมพิวเตอร์ที่สามารถอ่านได้ด้วยสายตาจึงจัดว่าเป็นต้นฉบับทั้งสิ้น แต่ทั้งนี้ "ต้นฉบับ" ดังกล่าวต้องเป็น

[1] Federal Rule of Evidence Act, article 1001.

> "ต้นฉบับ" ที่ Printout หรือ Disk ที่ได้จากคอมพิวเตอร์โดยตรงมิใช่การอัดสำเนาภายถ่าย หรือ Printout หรือ Disk ที่เกิดขึ้นจากการอัดสำเนา ซึ่งหลักการดังกล่าวแสดงให้เห็นว่าศาลแห่งสหรัฐอเมริกาได้ยอมรับการอ้างส่ง Printout หรือ Disk ให้เป็น "ต้นฉบับ" และเป็นพยานหลักฐานที่ดีที่สุดในการเสนอต่อศาลเพื่อพิสูจน์เนื้อหาที่บันทึกไว้ได้

อย่างไรก็ตามปัญหาในการพิจารณาในกรณี Printout หรือ Disk ว่า Printout หรือ Disk แบบใดจัดเป็นต้นฉบับ หรือแบบใดเป็นอัดสำเนา ซึ่งลักษณะของพยานหลักฐานดังกล่าวมีลักษณะพิเศษที่สามารถทำซ้ำได้ตลอดเวลาและไม่สามารถพิสูจน์ได้ว่า Printout หรือ Disk แผ่นใดเป็นต้นฉบับ หรืออัดสำเนา ซึ่งตามกฎหมายฉบับนี้ได้กำหนดให้ Printout หรือ Disk ที่ได้มาจากเครื่องคอมพิวเตอร์โดยตรงจึงเป็นต้นฉบับ รวมถึง Disk, Hard Disk หรือ Software ที่สามารถแสดงข้อมูลได้ทางจอภาพผ่านการประมวลผลของเครื่องคอมพิวเตอร์ จึงจัดเป็นต้นฉบับ แต่หากเป็น Printout หรือ Disk แบบอื่นใดที่สามารถสะท้อนข้อมูลในต้นฉบับ หรือถูกบันทึก หรือได้ถูกแก้ไขใหม่ก็ไม่อาจบังคับใช้ให้เป็นพยานหลักฐานที่ดีที่สุดได้

4.1.2 การรับฟังพยานหลักฐานตามหลัก Hearsay

โดยปกติแล้วตามหลักการรับฟังพยานหลักฐานตามหลัก Hearsay ซึ่งเป็นบทตัดพยานบอกเล่าให้มิอาจเป็นพยานหลักฐานที่รับฟังได้ ยกเว้นในกรณีซึ่ง

(1) เป็นความจำเป็นที่ไม่อาจอ้างพยานหลักฐานอื่นที่ได้อีกแล้ว กล่าวคือ การกล่าวของผู้ร้ายก่อนตาย

(2) พยานหลักฐานบางประเภทถึงแม้จะเป็น Hearsay ก็เชื่อถือได้ ยกตัวอย่าง เช่น คำกล่าวอันเป็นปฏิปักษ์ต่อตนเอง บันทึกที่ได้ทำโดยปกติทางธุรกิจหรือธนาคาร คำกล่าวที่ให้ไว้ต่อแพทย์ หรือกิติศัพท์เล่าลือในเขตที่ดิน เป็นต้น

โดยหากเป็นพยานหลักฐานที่มีลักษณะเช่นนี้ย่อมถือว่าสามารถใช้อ้างเป็นพยานหลักฐานได้ตามหลักข้อยกเว้นของหลัก Hearsay ประกอบกับการพิจารณาถึงข้อมูลทางคอมพิวเตอร์ หรือข้อมูลทางอิเล็กทรอนิกส์ที่ได้จากเครื่องหรือระบบคอมพิวเตอร์ และเป็นข้อมูลที่ได้จัดทำหรือบันทึกที่ได้จัดทำขึ้นโดยปกติแห่งทางธุรกิจย่อมถือว่าเป็นข้อยกเว้นของหลัก Hearsay ดังที่ได้อธิบายแล้วข้างต้น เนื่องจากข้อมูลที่ได้จัดทำหรือบันทึกทางคอมพิวเตอร์ หรือทางอิเล็กทรอนิกส์ที่ได้จัดทำหรือบันทึกโดยปกติแห่งทางธุรกิจนั้นถือเป็นพยานหลักฐาน ซึ่งจัดได้ว่า

เชื่อถือได้ และถือได้ว่าพยานหลักฐานดังกล่าวมีความถูกต้องและสมบูรณ์ ซึ่งสามารถใช้อ้างเป็นพยานหลักฐานต่อศาลได้ ตามหลักข้อยกเว้นของหลัก Hearsay

<u>หลักการรับฟังพยานหลักฐานทางคอมพิวเตอร์ตามข้อยกเว้นของหลัก Hearsay</u>

การรับฟังพยานหลักฐานตามหลักข้อยกเว้นของหลัก Hearsay ซึ่งหลักการดังกล่าวเป็นหลักกฎหมายคอมมอนลอว์ที่กำหนดเรื่องบทตัดพยานไว้ ซึ่งกำหนดให้ โดยทั่วไปพยานที่มีลักษณะเป็น Hearsay จะต้องห้ามรับฟังเสมอ เนื่องจากตามหลักการพิจารณาคดีของระบบกฎหมายคอมมอนลอว์มุ่งหมายให้คณะลูกขุนและศาลพิสูจน์ความจริงจากระบบการถามค้านพยานมากกว่าการรับฟังพยานที่นำเสนอต่อศาล โดยเชื่อว่าระบบการถามค้านเป็นระบบการพิสูจน์ความจริงที่มีประสิทธิภาพและสามารถพิสูจน์ความจริงได้มากกว่า ดังนั้น การห้ามรับฟังพยานหลักฐานที่เป็น Hearsay หรือหลักบทตัดพยาน ซึ่งเป็นหลักการพิจารณาการรับฟังพยานหลักฐานที่เป็น Hearsay

โดยพยานหลักฐานที่เป็น Hearsay หมายถึง คำกล่าวนอกศาล (out of court statement) ที่นำมาเสนอต่อศาลเพื่อมุ่งพิสูจน์ความจริงของคำกล่าวนั้น ซึ่งตามหลักการพิจารณาคดีของระบบกฎหมายคอมมอนลอว์กำหนดให้ห้ามรับฟังพยานหลักฐานดังกล่าว เว้นแต่กรณีพยานหลักฐานที่เข้าข้อยกเว้นของ Hearsay หรือที่เรียกว่า ข้อยกเว้นของบทตัดพยาน นอกจากนั้นตามหลักกฎหมายคอมมอนลอว์ถือว่าพยานเอกสารแทบทุกประเภทจัดเป็น Hearsay ทั้งสิ้น เพราะพยานเอกสารเป็นพยานที่ได้จัดทำขึ้นนอกศาล และแท้จริงแล้วพยานเอกสารดังกล่าวหมายถึง บันทึกคำบอกกล่าวของบุคคลซึ่งได้กระทำนอกศาลนั้นเอง ดังนั้นตามหลักการรับฟังพยานหลักฐานที่เป็น Hearsay ซึ่งต้องรวมถึงการรับฟังพยานหลักฐานที่เป็นพยานเอกสารด้วย ซึ่งหมายความว่า พยานเอกสารที่จะสามารถรับฟังได้ต้องเป็นพยานหลักฐาน เฉพาะกรณีที่เป็นข้อยกเว้นของ Hearsay หรือข้อยกเว้นของบทตัดพยานดังกล่าวเท่านั้น

ข้อยกเว้นของการรับฟังพยานหลักฐานที่เป็น Hearsay หรือข้อยกเว้นของบทตัดพยาน ได้กำหนดไว้ให้รับฟังพยานหลักฐานเฉพาะพยานหลักฐานบางประเภทเท่านั้น และเรียกได้ว่า “ข้อยกเว้นของบทตัดพยาน” นี้ เป็น “ข้อยกเว้นซ้อนข้อยกเว้น” ในการอนุญาตให้รับฟังพยาน Hearsay ได้เฉพาะใน 2 กรณี กล่าวคือ

1. ความจำเป็นเนื่องจากไม่มีพยานอื่นที่ดีกว่านี้แล้ว เช่น คำกล่าวของผู้ที่ใกล้ตาย เป็นต้น หรือ

2. ความน่าเชื่อถือของพยานบางประเภทที่มีลักษณะเป็น Hearsay แต่มีความน่าเชื่อถือว่าเป็นพยานหลักฐานที่ถูกต้องแท้จริง เช่น คำกล่าวอันเป็นส่วนหนึ่งของเหตุการณ์ คำกล่าวอันเป็นปฏิปักษ์ต่อตนเอง หรือบันทึกที่ทำโดยปกติในทางราชการหรือในทางธุรกิจ เป็นต้น

จากการศึกษาพยานหลักฐานที่เป็น Hearsay เปรียบเทียบพยานหลักฐานทางคอมพิวเตอร์ หรือพยานหลักฐานอิเล็กทรอนิกส์ซึ่งเป็นพยานหลักฐานที่ได้มาจากคอมพิวเตอร์ตามกฎหมายลักษณะพยานของประเทศสหรัฐอเมริกาจัดว่า พยานหลักฐานดังกล่าวเป็นพยานหลักฐานที่ดีที่สุด แต่หากพิจารณาถึงพยานหลักฐานทางคอมพิวเตอร์ หรือพยานหลักฐานทางอิเล็กทรอนิกส์ที่มิได้มาจากเครื่องคอมพิวเตอร์โดยตรง เช่น พยานหลักฐานที่เกิดขึ้นจากการจัดเก็บ แสดง หรือบันทึกใหม่หรือกระทำซ้ำ เช่นนี้ต้องถือว่าข้อมูลดังกล่าวมีลักษณะดังกล่าวจัดว่าเป็นพยานหลักฐานประเภท Hearsay และข้อมูลทางคอมพิวเตอร์หรือข้อมูลที่ได้จากอุปกรณ์อิเล็กทรอนิกส์ที่มาจากเครื่องคอมพิวเตอร์ที่มีการทำ เสนอ หรือบันทึกใหม่ หรือกระทำซ้ำ ซึ่งเป็นพยานหลักฐานประเภท Hearsay แต่เป็นข้อมูลที่ได้จากการบันทึกหรือจัดทำโดยปกติในทางธุรกิจ หรือไม่มีพยานหลักฐานอื่นที่ดีกว่านี้ กรณีดังกล่าวย่อมต้องถือว่าเป็นข้อยกเว้นแห่งหลัก Hearsay หรือข้อยกเว้นของหลักบทตัดพยาน โดยทำให้พยานหลักฐานประเภทนี้สามารถนำอ้างเป็นพยานหลักฐานต่อศาลที่สามารถรับฟังได้ตามหลักข้อยกเว้นของหลัก Hearsay หรือข้อยกเว้นของหลักบทตัดพยาน

4.1.3 การรับฟังพยานหลักฐานต้องอยู่ภายใต้หลักการรับรองความถูกต้องแท้จริง

นอกจากการพิจารณาถึงข้อมูลของเครื่องคอมพิวเตอร์ หรือข้อมูลทางอิเล็กทรอนิกส์ที่ได้มาจากเครื่องคอมพิวเตอร์ หรือมาจากการประมวลผลของเครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ ซึ่งกฎหมายลักษณะพยานแห่งประเทศสหรัฐอเมริกาถือว่าเป็น “ต้นฉบับ” และสามารถรับฟังเป็นพยานหลักฐานแห่งกฎหมายฉบับนี้ได้แล้ว การนำเสนอพยานหลักฐานดังกล่าวจะต้องนำเสนอประกอบการรับรองความถูกต้อง โดยพยานผู้เชี่ยวชาญหรือพยานผู้ที่เป็นเจ้าของข้อมูลที่ได้มาจากการประมวลผลของคอมพิวเตอร์ดังกล่าว

ซึ่งการนำเสนอพยานหลักฐานที่ได้มาจากการประมวลผลของคอมพิวเตอร์ที่ต้องนำสืบประกอบการรับรองความถูกต้องโดยพยานผู้เชี่ยวชาญ ด้วยเหตุว่า การนำเสนอพยานหลักฐาน ไม่ว่าจะเป็น Disk หรือ Printout นั้น พยานหลักฐานดังกล่าวมีลักษณะพิเศษ ซึ่งล้วนแล้วแต่ต้องการคำอธิบาย และความเข้าใจในระบบประกอบการพิจารณาความถูกต้องที่แท้จริงของ

พยานหลักฐานดังกล่าว ซึ่งพยานผู้เชี่ยวชาญจะเป็นผู้ที่มีความเชี่ยวชาญเกี่ยวกับพยานหลักฐานดังกล่าวและสามารถอธิบายหรือพิสูจน์ความถูกต้องแท้จริงของพยานหลักฐานประเภทนี้ได้ ไม่ว่าจะนำเสนอพยานหลักฐานประเภทใดมาอ้างอิงเป็นพยาน หรืออีกกรณีหนึ่งซึ่งเป็นการรับรองความถูกต้องที่แท้จริงของพยานหลักฐานดังกล่าว โดยกำหนดให้ผู้ดูแล หรืออาจหมายถึงผู้จัดการ ผู้ดูแล หรือผู้จัดทำข้อมูลภายใต้ระบบคอมพิวเตอร์หรือระบบการประมวลผลของข้อมูลดังกล่าว ซึ่งบุคคลนั้นต้องสามารถบรรยายรายละเอียดเกี่ยวกับระบบคอมพิวเตอร์ที่ใช้ทำการประมวลผลดังกล่าวได้อย่างละเอียด หรือเป็นบุคคลที่สามารถตรวจสอบได้ว่าระบบคอมพิวเตอร์ หรือการประมวลผลดังกล่าวได้ทำงานอย่างถูกต้องหรือไม่ เพื่อนำสืบประกอบในการรับรองความถูกต้องแท้จริงของพยานหลักฐานดังกล่าว

4.2 ข้อพิจารณาทางด้านการรับฟังพยานหลักฐานทางคอมพิวเตอร์ของประเทศสหราชอาณาจักร

ตามกฎหมายลักษณะพยานหลักฐานแห่งประเทศสหราชอาณาจักร ได้กำหนดถึงการรับฟังพยานหลักฐานทางคอมพิวเตอร์หรือพยานหลักฐานทางอิเล็กทรอนิกส์ ซึ่งมีข้อพิจารณาการรับฟังพยานหลักฐานอยู่หลายประการ ดังรายละเอียดสรุปได้ดังนี้

4.2.1 การรับฟังพยานหลักฐานตามกฎหมายลักษณะพยาน

การรับฟังพยานหลักฐานตามกฎหมายลักษณะพยานหลักฐาน (The Police and Criminal Evidence Act) ซึ่งได้บัญญัติไว้ในมาตรา 69 [2] กำหนดว่า ในกระบวนการพิจารณาคดีใดๆ ข้อความในเอกสารที่ทำขึ้นโดยคอมพิวเตอร์จะไม่เป็นการรับฟังในฐานะพยานหลักฐานตามข้อเท็จจริงที่ได้ระบุไว้

(a) ไม่มีเหตุอื่นอันควรเชื่อได้ว่าข้อความไม่ถูกต้อง อันเนื่องจากการใช้เครื่องคอมพิวเตอร์ไม่ถูกวิธี และ

(b) ตลอดระยะเวลาที่สำคัญนั้น คอมพิวเตอร์ได้ปฏิบัติการอย่างถูกต้องและแม้หากมีกรณีทำงานของเครื่องขัดข้องก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

ดังนั้น จากหลักการรับฟังพยานหลักฐานทางคอมพิวเตอร์ของประเทศสหราชอาณาจักรดังกล่าว จะเห็นได้ว่า การนำข้อมูลทางคอมพิวเตอร์หรือข้อมูลทางอิเล็กทรอนิกส์ที่ได้มาจากเครื่องหรือระบบคอมพิวเตอร์เพื่อนำเสนอเป็นพยานหลักฐานแห่งคดีตามมาตรา 69 นี้ต้องเป็น

[2] The Police and Criminal Evidence Act, section 69.

พยานหลักฐานที่เป็นไปตามข้อยกเว้นที่กำหนดไว้ในมาตรา 69 (a) และ (b) ซึ่งจะถือว่าเป็นพยานหลักฐานที่สามารถรับฟังได้ ซึ่งข้อยกเว้นดังกล่าวมีหลักเกณฑ์ ดังต่อไปนี้

(1) ไม่มีเหตุผลอื่นใดอันควรเชื่อได้ว่าข้อความไม่ถูกต้อง อันเนื่องมาจากการใช้เครื่องคอมพิวเตอร์ไม่ถูกวิธี

(2) ตลอดระยะเวลา คอมพิวเตอร์ได้ปฏิบัติการอย่างถูกต้อง และแม้ว่าเครื่องคอมพิวเตอร์ขัดข้องก็ไม่เป็นการกระทบถึงข้อมูลดังกล่าว

4.2.2. การรับฟังพยานหลักฐานต้องมีการรับรองเอกสาร

ตามกฎหมายลักษณะพยาน (The Police and Criminal Evidence Act) ตามที่บัญญัติไว้ในมาตรา 68 [3] ได้กำหนดถึงการรับฟังพยานหลักฐานทางคอมพิวเตอร์ ซึ่งกำหนดให้พยานหลักฐานที่ใช้อ้างเป็นพยานหลักฐานในคดีต้องมีใบรับรอง และใบรับรองดังกล่าวต้องมีรายละเอียดดังนี้

(1) พิสูจน์เอกสารที่บรรจุข้อความและอธิบายวิธีการรักษา

(2) ให้รายละเอียด โดยอธิบายให้เห็นว่าข้อมูลถูกทำขึ้นโดยเครื่องคอมพิวเตอร์

(3) ข้อความดังกล่าวได้รับการลงนามจากบุคคลที่ดำรงตำแหน่งและมีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการใช้คอมพิวเตอร์นั้น

4.2.3 กำหนดลักษณะของพยานหลักฐานทางคอมพิวเตอร์ตามความหมายของคำว่า “คอมพิวเตอร์” ตามกฎหมายลักษณะพยาน

ตามกฎหมายลักษณะพยานแห่งประเทศสหราชอาณาจักร (The Police and Criminal Evidence Act) ได้กำหนดความหมายของคำว่า “คอมพิวเตอร์” ซึ่งกำหนดว่า วัสดุหรืออุปกรณ์ใดๆ ที่ใช้สำหรับการเก็บ ประมวลผลข้อมูลและการอ้างถึงข้อมูลใดๆ ที่ได้มาจากอีกข้อมูลหนึ่ง และให้รวมถึงการคิดคำนวณ การเปรียบเทียบ หรือขบวนการใดๆ จากข้อมูลนั้นๆ

ซึ่งหากพิจารณาจากประเด็นที่กล่าวข้างต้น จะเห็นได้ว่า กฎหมายแห่งประเทศสหราชอาณาจักรยอมรับให้ข้อมูลทางคอมพิวเตอร์ หรือข้อมูลทางอิเล็กทรอนิกส์ที่ได้มา

---

[3] The Police and Criminal Evidence Act, section 68.

จากคอมพิวเตอร์สามารถรับฟังเป็นพยานหลักฐานได้ โดยมิได้มีข้อจำกัดเกี่ยวกับการรับฟังพยานหลักฐานที่ดีที่สุดมาบังคับใช้กับกรณีดังกล่าว หากแต่พยานหลักฐานทางคอมพิวเตอร์หรือพยานหลักฐานทางอิเล็กทรอนิกส์ดังกล่าวต้องถูกจำกัดให้ต้องมีคำรับรองยืนยันความถูกต้องในการทำงานของเครื่องคอมพิวเตอร์ดังกล่าวไว้จากผู้ที่เกี่ยวข้องกับการใช้เครื่องคอมพิวเตอร์นั้นหรือผู้ซึ่งหน้าที่รับผิดชอบที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์นั้น

4.2.4 ผลลัพธ์จากเครื่องคอมพิวเตอร์โดยตรงจัดเป็นพยานบอกเล่า

พยานหลักฐานซึ่งเป็นผลลัพธ์จากเครื่องคอมพิวเตอร์โดยตรงจัดเป็นพยานบอกเล่าและการรับฟังพยานหลักฐานดังกล่าวต้องเป็นไปตามหลัก Hearsay ซึ่งเป็นหลักบทตัดพยานหรือหลักการห้ามรับฟังพยานบอกเล่า

โดยส่วนใหญ่กฎหมายทั่วไปมักจะกำหนดให้ผลลัพธ์ของเครื่องคอมพิวเตอร์หรือที่มิได้มาจากเครื่องคอมพิวเตอร์โดยตรงจัดเป็นพยานบอกเล่า ตามหลักการรับฟังพยานหลักฐานประเภท Hearsay ตามกฎหมายลักษณะพยานแห่งประเทศสหรัฐอเมริกา ซึ่งหลักการดังกล่าวกำหนดให้ข้อมูลที่มิได้มาจากเครื่องคอมพิวเตอร์โดยตรงมีฐานะเป็นพยานบอกเล่า และจะรับฟังได้กรณีที่เข้าข้อยกเว้นของหลัก Hearsay ซึ่งไม่อาจหาพยานหลักฐานอื่นที่ดีกว่าได้ หรือเป็นพยานที่มีความน่าเชื่อถือซึ่งเป็นพยานหลักฐานที่ได้มาจากกระบวนทางคอมพิวเตอร์โดยปกติทางธุรกิจ

แต่กฎหมายแห่งประเทศสหราชอาณาจักรได้กำหนดให้ ผลลัพธ์จากเครื่องคอมพิวเตอร์บางประเภทมีฐานะเป็นพยานบอกเล่า แม้ว่าจะเป็นพยานหลักฐานโดยตรงจากคอมพิวเตอร์ เช่น ผลลัพธ์จากคอมพิวเตอร์ที่ใช้ในการคำนวณหรือประมวลผล เนื่องจากเป็นการทำงานของเครื่องคอมพิวเตอร์โดยตรง แต่ผลลัพธ์ที่ได้ดังกล่าวมิได้ยืนยันถึงความจริงเกี่ยวกับพยานบุคคลที่มิได้มาในศาลจึงจัดเป็นพยานบอกเล่า และสามารถรับฟังได้เฉพาะกรณีข้อยกเว้นของหลัก Hearsay แต่หากเป็นกรณีที่เป็น Printout หรือ Disk ที่เป็นข้อมูลที่ได้จากคอมพิวเตอร์ต้นแบบถือได้ว่าเป็นผลลัพธ์ของคอมพิวเตอร์โดยตรง และจัดเป็นพยานหลักฐานที่มีฐานะเป็นพยานโดยตรงมิใช่พยานบอกเล่า

4.2.4 การนำสืบพยานหลักฐานทางคอมพิวเตอร์

การนำสืบพยานหลักฐานทางคอมพิวเตอร์ต้องใช้พยานบุคคล ซึ่งเป็นบุคคลที่สามารถพิสูจน์ข้อมูลและอธิบายวิธีการรักษา หรือสามารถให้รายละเอียดโดยอธิบายให้เห็นว่า

ข้อมูลถูกทำขึ้นโดยเครื่องคอมพิวเตอร์ หรือบุคคลที่ตำแหน่งและมีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการใช้คอมพิวเตอร์นั้นเป็นพยานผู้เชี่ยวชาญในการนำสืบและอธิบายถึงการทำงานของเครื่องคอมพิวเตอร์โดยไม่ติดขัดกับหลักการรับฟังพยานบอกเล่าดังกล่าวนั้นแต่อย่างใด

บทที่ 5

บทสรุปและข้อเสนอแนะ

หากกล่าวถึงการโอนเงินทางอิเล็กทรอนิกส์นั้นมิใช่การกระทำที่เป็นความผิด หรือการกระทำที่เป็นอันตราย หรือเป็นอาชญากรรมที่สร้างความเสียหายให้แก่บุคคลหนึ่งบุคคลใด องค์กร หรือประเทศชาติได้ แต่การโอนเงินทางอิเล็กทรอนิกส์เป็นกระบวนการหนึ่งในการชำระเงินหรือเป็นกระบวนการในการทำธุรกรรมทางการเงินการธนาคารอย่างหนึ่ง เพื่ออำนวยความสะดวกทางการเงินการธนาคารให้แก่ผู้ใช้บริการ หรือธุรกิจการค้าการพาณิชย์ภายในประเทศหรือการค้าระหว่างประเทศ อาจไม่มีใครมองได้เลยว่าการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าวจะสามารถสร้างความเสียหายหรือเป็นการกระทำอันเป็นความผิดทางอาญาได้อย่างไร

แต่ในปัจจุบัน ภัยจากอาชญากรทางเศรษฐกิจที่นำเอาระบบการโอนเงินอิเล็กทรอนิกส์ ซึ่งเป็นระบบในการอำนวยความสะดวกและให้บริการทางการเงินการธนาคารให้แก่ผู้ใช้บริการ และธุรกิจการค้าการพาณิชย์ต่างๆ มาเป็นเครื่องมือในการกระทำความผิด หรือกระทำทุจริตทางคอมพิวเตอร์ต่อระบบการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าว ซึ่งประเทศไทยควรมีมาตรการทางกฎหมายในการบังคับใช้กับการกระทำความผิดดังกล่าว มิใช่หากแต่เพียงมาตรการในการบังคับใช้และลงโทษผู้กระทำความผิดเท่านั้น แต่มาตรการทางกฎหมายดังกล่าวยังต้องมีมาตรการในการแก้ไขเยียวยา หรือหยุดยั้งความเสียหายที่เกิดขึ้น ไม่ว่าจะเป็นต่อบุคคล นิติบุคคล สถาบันทางการเงิน ธนาคารพาณิชย์ หรือประเทศ ซึ่งประเทศไทยยังมีปัญหาในการบังคับใช้กฎหมายกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าว ตั้งแต่บทบัญญัติในการกำหนดลักษณะความผิด บทกำหนดโทษ รวมไปถึงการพิสูจน์ถึงความผิดตามหลักการรับฟังพยานหลักฐานซึ่งกรณีนี้เป็นพยานหลักฐานทางอิเล็กทรอนิกส์ ตลอดจนการริบทรัพย์สินซึ่งเป็นทรัพย์สินที่ได้มาจากกระทำความผิดดังกล่าว หรือได้มาจากความผิดอื่นแต่อาศัยกระบวนการโอนเงินทางอิเล็กทรอนิกส์เป็นเครื่องมือการปิดบังที่มาของทรัพย์สินดังกล่าว เพื่อหยุดยั้งหรือลงโทษต่อการกระทำความผิดดังกล่าว

จากการศึกษาความผิดเกี่ยวกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ภายใต้มาตรการทางกฎหมายในต่างประเทศดังที่ได้อธิบายแล้วข้างต้นจะเห็นได้ว่ามีแนวทางในการบังคับใช้มาตรการทางกฎหมายต่ออาชญากรรมที่เกิดขึ้นในการโอนเงินทางอิเล็กทรอนิกส์ โดยมีรายละเอียดซึ่งสรุปได้ ดังนี้

<u>ประการแรก</u> แนวทางในการคุ้มครองกระบวนการโอนเงินทางอิเล็กทรอนิกส์ให้เป็นไปในแนวทางการป้องกันและปราบปรามอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ โดยการกำหนดหลักปฏิบัติที่ถูกต้องและเหมาะสมในการโอนเงินทางอิเล็กทรอนิกส์ให้ผู้โอน สถาบันทางการเงิน ธนาคาร หรือบุคคลที่เกี่ยวข้องมีภาระหน้าที่ต้องปฏิบัติตามหลักเกณฑ์ของการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าว นอกเหนือจากนั้นมาตรการทางกฎหมายดังกล่าวยังมีกำหนดลักษณะความผิดทางอาญาในกรณีที่ผู้โอน สถาบันทางการเงิน ธนาคาร หรือบุคคลที่เกี่ยวข้องไม่ปฏิบัติตามหลักเกณฑ์ดังกล่าว ซึ่งการกำหนดลักษณะความผิดดังกล่าวเป็นส่วนหนึ่งของการบังคับใช้ให้มาตรการทางกฎหมายดังกล่าวสามารถบังคับใช้ได้อย่างมีประสิทธิภาพ และเป็นรูปธรรม

<u>ประการที่สอง</u> แนวทางในการกำหนดถึงลักษณะของการกระทำความผิดที่เป็นอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ไว้โดยเฉพาะ

<u>ประการที่สาม</u> แนวทางในการกำหนดมาตรการในการลงโทษขั้นสูงหรือกำหนดเพิ่มโทษ ไม่ว่าจะเป็นโทษปรับหรือโทษจำคุก สำหรับความผิดที่เกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์บางลักษณะความผิด ซึ่งเป็นความผิดที่มีผลกระทบ หรือสร้างความเสียหายให้แก่สถาบันทางการเงินหรือระบบการเงินการธนาคารของประเทศ

<u>ประการที่สี่</u> แนวทางในการกำหนดให้ใช้มาตรการริบทรัพย์สินในการใช้บังคับกับการกระทำความผิดที่เกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นมาตรการริบทรัพย์สินทางแพ่งอันเป็นการยึดทรัพย์สิน ซึ่งใช้บังคับในการริบทรัพย์สินดังกล่าวก่อนมีคำพิพากษาที่พิสูจน์ได้ว่าเป็นทรัพย์สินที่เกี่ยวข้อง ได้มา หรือได้ประโยชน์จากกระบวนการโอนเงินทางอิเล็กทรอนิกส์ หรือทรัพย์สินที่เกี่ยวข้อง หรือได้มาจากการกระทำความผิดอื่นๆ แต่อาศัยกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในการปกปิดที่มาแห่งทรัพย์สินดังกล่าว ซึ่งเป็นการแก้ไขเยียวยาและหยุดยั้งการกระทำความผิดดังกล่าวหรือความเสียหายที่เกิดขึ้นได้ในระดับหนึ่ง

รวมถึงมาตรการริบทรัพย์สินทางอาญาที่กำหนดให้รัฐสามารถทำการริบทรัพย์สินที่เกี่ยวข้อง ได้มา หรือได้ประโยชน์จากกระบวนการโอนเงินทางอิเล็กทรอนิกส์ หรือทรัพย์สินที่เกี่ยวข้อง หรือได้มาจากการกระทำความผิดอื่น ๆ แต่อาศัยกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในการปกปิดที่มาแห่งทรัพย์สินดังกล่าวซึ่งให้เป็นไปตามคำพิพากษาของศาล เพื่อเป็นบทลงโทษแก่ผู้กระทำความผิดดังกล่าว

<u>ประการที่ห้า</u> แนวทางในการกำหนดให้มาตรการริบทรัพย์สินมีผลใช้บังคับย้อนหลัง เพื่อเป็นการติดตามหรือสืบเสาะทรัพย์สินที่เกี่ยวข้อง ได้มา หรือได้ประโยชน์จากกระบวนการโอนเงินทางอิเล็กทรอนิกส์ หรือทรัพย์สินที่เกี่ยวข้อง หรือได้มาจากการกระทำความผิดอื่นๆ แต่อาศัยกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในการปกปิดที่มาแห่งทรัพย์สินดังกล่าว

ซึ่งพิจารณาจากบทบัญญัติแห่งมาตรการริบทรัพย์สินที่มีการกำหนดให้มีการสืบเสาะทรัพย์สินที่ต้องถูกริบได้ จึงเป็นบทยกเว้นแห่งหลักทั่วไปของกฎหมายอาญาซึ่งไม่มีผลใช้บังคับย้อนหลัง โดยมาตรการริบทรัพย์สินดังกล่าวให้อำนาจแก่เจ้าพนักงานที่มีอำนาจหน้าที่สามารถสืบเสาะ และติดตาม รวมทั้งทำการริบทรัพย์สินที่ต้องถูกริบได้ ณ ปัจจุบันย้อนหลังไปจนถึงขณะกระทำความผิดได้

<u>ประการที่หก</u> แนวทางในการกำหนดหน่วยงานพิเศษที่มีอำนาจหน้าที่เฉพาะเพื่อบังคับใช้กฎหมายกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าว ซึ่งถือเป็นความผิดที่มีลักษณะพิเศษเฉพาะ โดยหน่วยงานเฉพาะดังกล่าวอาจถูกกำหนดขึ้นเพื่อทำหน้าที่ในการสืบสวนสอบสวนการกระทำความผิดต่อระบบโอนเงินทางอิเล็กทรอนิกส์ หรือทำหน้าที่ในการตรวจสอบ หรือสืบเสาะข้อมูลทางการเงินที่อาจเกี่ยวข้องกับการกระทำความผิด ที่เกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ รวมไปจนถึงการทำหน้าที่ในการตรวจสอบเพื่อป้องกันและปราบปรามความผิดฐานฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ หรือเก็บรวบรวมข้อมูล ที่เกี่ยวข้อง หรืออาจเป็นพยานหลักฐานเกี่ยวกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ หรือเป็นข้อมูลสนับสนุนหน่วยงานที่บังคับใช้กฎหมายหรือมีอำนาจหน้าที่ในการสืบสวนสอบสวนคดีดังกล่าว ซึ่งกระบวนการเหล่านี้ล้วนแล้วแต่ต้องอาศัยความรู้ความเชี่ยวชาญทางด้านอิเล็กทรอนิกส์และระบบการโอนเงินทางอิเล็กทรอนิกส์โดยเฉพาะ ซึ่งหน่วยงานพิเศษดังกล่าวจะจัดให้มีพนักงานเจ้าหน้าที่ซึ่งมีความเชี่ยวชาญเฉพาะด้านทางด้านการเงินการธนาคารหรือเทคโนโลยีเฉพาะในการทำหน้าที่สืบสวนสอบสวนคดีดังกล่าว และมีการพัฒนาความรู้ทางด้านเทคโนโลยีคอมพิวเตอร์ หรือระบบทางอิเล็กทรอนิกส์ที่เกี่ยวข้องกับระบบการเงินการธนาคารอยู่เสมอ

<u>ประการที่เจ็ด</u> แนวทางในการกำหนดเขตอำนาจรัฐพิเศษ ซึ่งบางลักษณะความผิดอาจเกิดการขัดกันทางด้านเขตอำนาจแห่งรัฐ ซึ่งอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินระหว่างประเทศจะเห็นได้ว่าความผิดที่เกิดขึ้นอยู่ภายใต้เขตอำนาจแห่งรัฐหลายรัฐและมาตรการทางกฎหมายต่างประเทศบางประเทศได้กำหนดให้ ถือว่าเป็นความผิดที่อยู่ภายใต้เขตอำนาจแห่งรัฐ กล่าวคือ

1. หากการกระทำความผิดที่เกิดขึ้นเพียงส่วนหนึ่งส่วนใดแห่งรัฐ หรือการกระทำความผิดที่เกิดขึ้นนอกเขตอำนาจรัฐ แต่ความผิดกลับมีผลกระทบต่อรัฐ ความผิดเหล่านี้ให้ถือว่าเป็นการกระทำความผิดในเขตอำนาจแห่งรัฐ
2. หากผู้การกระทำความผิดต่อรัฐ แต่อาจถูกจับหรือถูกกักขังในต่างประเทศก็ให้ถือว่าเป็นความผิดในเขตอำนาจแห่งรัฐ
3. หากการกระทำความผิดที่เกิดขึ้นนอกเขตอำนาจรัฐ หากแต่เป็นการกระทำของบุคคลในรัฐ ถือว่าอยู่ในเขตอำนาจรัฐ

ประการที่แปด แนวทางในการกำหนดมาตรการในการริบทรัพย์สิน ซึ่งกำหนดให้ มีความร่วมมือในระดับระหว่างประเทศในการริบทรัพย์สินที่เกี่ยวข้องกับความผิดฐานฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งตามอนุสัญญาแห่งสหภาพยุโรปว่าด้วยการค้น การยึดและริบทรัพย์สินที่ได้จากการประกอบอาชญากรรม (Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime) ซึ่งการริบทรัพย์สินดังกล่าวได้ถูกกำหนดขึ้นให้เป็นความร่วมมือในระดับระหว่างประเทศ โดยกำหนดให้รัฐที่มีอำนาจริบทรัพย์สินที่ต้องถูกริบและอยู่ภายใต้เขตอำนาจแห่งรัฐอื่น รัฐดังกล่าวอาจทำการร้องขอให้รัฐที่มีเขตอำนาจแห่งรัฐเหนือทรัพย์สินดังกล่าวเป็นผู้ริบทรัพย์สินนั้น และรัฐที่ถูกร้องขอจะทำการริบทรัพย์สินดังกล่าวได้ในกรณีที่มีการตรวจสอบความถูกต้องหรืออำนาจแห่งรัฐที่ร้องขอว่าถูกต้องครบถ้วนเป็นที่เรียบร้อยแล้ว

ประการที่เก้า แนวทางในการกำหนดความรับผิดทางแพ่งต่อรัฐ นอกเหนือจากโทษปรับหรือโทษจำคุกที่กำหนดไว้เป็นการทั่วไป สำหรับบางลักษณะความผิดซึ่งมีผลกระทบต่อรัฐหรือมาตรการด้านความปลอดภัยแห่งรัฐ ซึ่งรวมถึงมาตรการด้านความปลอดภัยในระบบการเงินการธนาคาร

ซึ่งจากบทวิเคราะห์แนวทางหรือมาตรการทางกฎหมายในต่างประเทศข้างต้น จะเห็นได้ว่า มีหลักการสำคัญที่กำหนดไว้ในมาตรการทางกฎหมายที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งผู้เขียนเห็นว่าควรนำมาเป็นแนวทางในการปรับปรุงกฎหมายของประเทศไทยต่อไป โดยมีหลักการและข้อเสนอแนะดังต่อไปนี้

5.1 แนวทางในการบัญญัติกฎหมายกำหนดลักษณะความผิด

การวางแนวทางในการบัญญัติกฎหมายในการกำหนดลักษณะความผิด และกำหนดโทษแก่ความผิดซึ่งเป็นอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ และการวางแนวทางในการบัญญัติกฎหมายดังกล่าว เพื่อบังคับใช้ให้ครอบคลุมกับความผิดลักษณะต่างๆ

หากพิจารณาถึงความพยายามในการร่างกฎหมาย เพื่อบังคับใช้กับอาชญากรรมทางคอมพิวเตอร์ในการโอนเงินทางอิเล็กทรอนิกส์ของไทยในปัจจุบัน ซึ่งจะเห็นได้จากร่างกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ภายใต้โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศของสำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ซึ่งขณะนี้ร่างกฎหมายดังกล่าวอยู่ระหว่างการนำเสนอคณะรัฐมนตรีเพื่อพิจารณา รวมถึงความพยายามในการแก้ไขเพิ่มเติมประมวลกฎหมายอาญาของคณะกรรมการกฤษฎีกา ในการยกร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่....) พ.ศ..... ที่กำหนดความผิดที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ไว้ เพื่อการบังคับใช้กับความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ซึ่งคณะรัฐมนตรีได้ลงมติเมื่อวันที่ 24 ธันวาคม 2545 โดยเห็นควรให้นำบทบัญญัติแห่งร่างกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ของสำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติดังกล่าวมาปรับลักษณะฐานความผิดดังกล่าวไว้ โดยให้ร่วมกันศึกษาและพิจารณากฎหมายฉบับดังกล่าวต่อไป

อย่างไรก็ตาม ผู้ศึกษาเห็นว่า การกำหนดมาตรการทางกฎหมายในการกำหนดลักษณะความผิดเพื่อบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์มีจุดมุ่งหมายสำคัญในการสร้างแนวทางของการคุ้มครองระบบโอนเงินทางอิเล็กทรอนิกส์ให้มีความปลอดภัยมากขึ้น ทั้งนี้ ควรนำแนวทางทางด้านกฎหมายในการคุ้มครองกระบวนการโอนเงินทางอิเล็กทรอนิกส์ของพระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ (Electronic Funds Transfer Act) และความผิดลักษณะต่างๆ ที่เกี่ยวข้องกับกระบวนการโอนเงินทางอิเล็กทรอนิกส์ที่กำหนดไว้ในประมวลกฎหมายอาญา (Federal Crime and Criminal Procedure) หรือพระราชบัญญัติต่อต้านการ

ฟอกเงินระหว่างประเทศและต่อต้านการก่อการร้าย ซึ่งกำหนดไว้ในพระราชบัญญัติการต่อต้านการก่อการร้าย (International Money Laundering Abatement Act : IMLA, in part of, USA Patriot Act, 2001) รวมถึงกฎหมายลักษณะดังกล่าวของประเทศสหราชอาณาจักร ซึ่งกำหนดไว้ในพระราชบัญญัติธนาคารแห่งสหราชอาณาจักร (The Bank of England Act, 1988) หรือพระราชบัญญัติว่าด้วยการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceeds of Crime,2002) หรือฐานความผิดต่าง ๆ ของการกระทำความผิดอันเป็นอาชญากรรมทางคอมพิวเตอร์ ซึ่งกำหนดไว้ในพระราชบัญญัติการกระทำโดยมิชอบต่อคอมพิวเตอร์ (The Computer Misuse Act) ลักษณะเดียวกับอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime) ของสภาสหภาพยุโรป (Council of Europe) ที่ได้วางแนวทางไว้ให้แก่ประเทศสมาชิกแห่งสหภาพยุโรป ซึ่งผู้ศึกษาได้อธิบายไว้แล้วในบทที่ 3 โดยนำฐานความผิดลักษณะต่างๆ ที่ได้อธิบายไว้ข้างต้นมาปรับใช้ และปรับปรุงแก้ไขเพิ่มเติมกฎหมายของประเทศไทยต่อไป

5.2 แนวทางในการบังคับใช้มาตรการในการริบทรัพย์สิน

จากการศึกษา แนวทางด้านกฎหมาย Federal Crime and Criminal Procedure ของสหรัฐอเมริกา ที่กำหนดมาตรการในการริบทรัพย์สินทางแพ่ง และทรัพย์สินทางอาญาในบางลักษณะความผิด รวมถึงอนุสัญญาว่าด้วยการค้น การยึด และริบทรัพย์สินที่ได้มาจากการกระทำความผิด (Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime) ซึ่งจะเห็นได้ว่ามาตรการริบทรัพย์สินดังกล่าวเป็นมาตรการในการแก้ไขเยียวยา และหยุดยั้งความเสียหาย รวมถึงชดเชยความเสียหายให้แก่ผู้เสียหาย ไม่ว่าจะเป็นบุคคล นิติบุคคล สถาบันทางการเงิน หรือรัฐ และเป็นมาตรการในการลงโทษขั้นรุนแรงแก่ผู้กระทำความผิดดังกล่าว กล่าวคือ

5.2.1 มาตรการริบทรัพย์สินดังกล่าวจะริบทรัพย์สินที่แท้จริง หรือทรัพย์สินส่วนตัวของผู้กระทำความผิด ตามจำนวนแห่งทรัพย์สินที่ได้มาหรือกระทำความผิดดังกล่าว หรือตามจำนวนที่กฎหมายกำหนด

5.2.2 ทรัพย์สินที่ต้องริบตามกฎหมายดังกล่าวนอกจากเป็นทรัพย์สินที่ได้มาหรือเป็นทรัพย์สินที่ใช้ในกระทำความผิดแล้ว และขณะที่การสืบสวนสอบสวนอาจไม่มีทรัพย์สินดังกล่าวอยู่ในการครอบครองของผู้กระทำความผิด เช่นในบางกรณีผู้กระทำความผิดอาจจำหน่าย จ่าย โอนทรัพย์สิน

ดังกล่าว เจ้าพนักงานมีอำนาจสืบเสาะทรัพย์สินดังกล่าวได้

5.2.3 มาตรการริบทรัพย์สินแบ่งได้เป็น มาตรการริบทรัพย์สินทางแพ่งและมาตรการริบทรัพย์สินทางอาญา ซึ่งมีลักษณะที่แตกต่างกัน กล่าวคือ

5.2.3.1 มาตรการริบทรัพย์สินทางแพ่งควรกระทำได้ทันทีที่หน่วยงานที่มีอำนาจหน้าที่ และได้สืบสวนสอบสวนกรณีดังกล่าวและเห็นว่าทรัพย์สินดังกล่าว เป็นทรัพย์สินที่กฎหมายได้กำหนดไว้ให้ริบผู้มีอำนาจนั้นสามารถร้องขอให้ศาลสั่งยึดทรัพย์สินดังกล่าวได้ทันทีก่อนศาลมีคำพิพากษาตัดสินว่าผู้นั้นกระทำความผิดจริงหรือไม่

5.2.3.2 มาตรการริบทรัพย์สินทางอาญาเป็นมาตรการริบทรัพย์สินที่ศาลมีคำพิพากษาลงโทษผู้กระทำความผิด โดยให้ริบทรัพย์สินนั้นตามจำนวนที่กระทำความผิด

5.2.4 มาตรการริบทรัพย์สินทางแพ่งเป็นมาตรการริบทรัพย์สินโดยมีวัตถุประสงค์เพื่อป้องกันการจำหน่าย จ่าย โอนทรัพย์สินดังกล่าวโดยผู้กระทำความผิด และการหยุดยั้งการกระทำความผิด หรือมีวัตถุประสงค์ในการชดเชยความเสียหายให้แก่ผู้เสียหายไม่ว่าจะเป็น รัฐ สถาบันทางการเงิน นิติบุคคลอื่นๆ

5.2.5 มาตรการริบทรัพย์สินทางอาญาเป็นมาตรการริบทรัพย์สินให้แก่รัฐ

5.2.6 แนวทางด้านกฎหมายที่บังคับใช้ในการใช้มาตรการริบทรัพย์สินต้องกระทำการสืบสวนสอบสวนโดยหน่วยงานที่มีความเชี่ยวชาญเฉพาะ และกฎหมายได้กำหนดไว้เป็น

พิเศษ เพื่อให้การบังคับใช้กฎหมายเป็นไปได้อย่างประสิทธิภาพ

จากการศึกษาผู้ศึกษาเห็นว่า ความผิดที่เป็นอาชญากรรมคอมพิวเตอร์ในการโอนเงินทางอิเล็กทรอนิกส์หรือการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์ นอกจากมาตรการในการกำหนดลักษณะความผิดและบทลงโทษความผิดดังกล่าวแล้ว ควรมีการกำหนดมาตรการในการริบทรัพย์สินทางแพ่งไว้เพื่อเป็นการคุ้มครองระบบการโอนเงินทางอิเล็กทรอนิกส์ในการหยุดยั้งการกระทำความผิด แก้ไขเยียวยาความเสียหายที่เกิดขึ้นเป็นเบื้องต้น หรือให้ยึดทรัพย์สินนั้นไว้เพื่อความปลอดภัยแก่ระบบโอนเงินทางอิเล็กทรอนิกส์ทันทีที่มีเหตุสงสัย และเมื่อได้รับการสืบสวนสอบสวนโดยหน่วยงานที่มีความเชี่ยวชาญเฉพาะแล้ว เห็นว่าต้องยึดทรัพย์สินดังกล่าวเพื่อความปลอดภัยแห่งทรัพย์สินนั้นว่า ทรัพย์สินนั้นได้มา ได้ประโยชน์หรือเกี่ยวข้องกับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์

นอกจากนั้น อาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าวยังควรมีมาตรการในการริบทรัพย์สินทางอาญา เพื่อเป็นการลงโทษขั้นสูงหรือการลงโทษอย่างรุนแรงแก่ผู้กระทำความผิด ซึ่งเป็นมาตรการในการกำหนดบทลงโทษเพื่อข่มขู่หรือทำให้เกรงกลัวต่อการกระทำความผิด ซึ่งมาตรการในการริบทรัพย์สินดังกล่าวสามารถริบทรัพย์สินที่ได้มา หรือได้ประโยชน์ หรือเกี่ยวข้องกับการกระทำความผิด ไม่ว่าจะยังคงอยู่ในสถานะเดิมหรือได้มีการเปลี่ยนแปลงความมีอยู่ของทรัพย์สินนั้นแล้ว รวมไปจนถึงทรัพย์สินส่วนตัวหรือทรัพย์สินใดๆ ของผู้กระทำความผิด เพื่อให้รัฐหรือผู้เสียหายกรณีดังกล่าวได้รับการชดเชยความเสียหายที่เกิดขึ้นแก่ระบบโอนเงินทางอิเล็กทรอนิกส์ดังกล่าวตามจำนวนที่เกิดขึ้น หรืออาจมากกว่านั้น

5.3 แนวทางในการรับฟังพยานหลักฐานทางคอมพิวเตอร์

ผู้ศึกษาเห็นว่า อาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์เป็นการกระทำที่เกี่ยวเนื่องกับระบบอิเล็กทรอนิกส์โดยตรง ดังนั้น พยานหลักฐานที่เกิดขึ้นในการพิสูจน์ความผิดย่อมเป็นพยานหลักฐานที่เกิดขึ้นจากระบบอิเล็กทรอนิกส์หรือระบบคอมพิวเตอร์ ทั้งนี้ เพื่อให้การบังคับใช้กฎหมายเป็นไปอย่างมีประสิทธิภาพและขจัดปัญหาในการตีความด้านการรับฟังพยานหลักฐานทางคอมพิวเตอร์หรือการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ จึงควรกำหนดมาตรการทางกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานทางคอมพิวเตอร์ หรือพยานหลักฐานทางอิเล็กทรอนิกส์ไว้ให้ชัดเจน ซึ่งควรมีการปรับปรุงและ

กำหนดมาตรการในรับฟังพยานหลักฐานดังกล่าวไว้ในกฎหมายที่บังคับใช้กับการโอนเงินทางอิเล็กทรอนิกส์ไว้

หากพิจารณาเปรียบเทียบหลักการรับฟังพยานหลักฐานในต่างประเทศ ไม่ว่าจะประเทศสหรัฐอเมริกา หรือประเทศสหราชอาณาจักรได้กำหนดหลักการรับฟังพยานหลักฐานทางคอมพิวเตอร์ หรือพยานหลักฐานทางอิเล็กทรอนิกส์เป็นพยานหลักฐานโดยตรง ซึ่งการรับฟังพยานหลักฐานเป็นไปตามหลักการรับฟังพยานหลักฐานที่ดีที่สุด (Best of evidence) แต่หากเป็นพยานหลักฐานทางคอมพิวเตอร์ หรือพยานหลักฐานทางอิเล็กทรอนิกส์ที่มิได้เป็นผลลัพธ์จากเครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์โดยตรง การรับฟังพยานหลักฐานย่อมเป็นไปตามข้อยกเว้นกรณีหากไม่อาจหาพยานหลักฐานใดที่ดีกว่าได้ หรือพยานหลักฐานดังกล่าวมีความน่าเชื่อถือด้วยเป็นพยานหลักฐานที่ได้มาจากการจัดการหรือการบันทึกโดยปกติทางธุรกิจ ซึ่งสามารถรับฟังเป็นพยานหลักฐานตามข้อยกเว้นของหลัก Hearsay

ซึ่งหากพิจารณาถึงข้อพิจารณาเกี่ยวกับการรับฟังพยานหลักฐาน ซึ่งเป็นข้อมูลทางคอมพิวเตอร์หรือข้อมูลทางอิเล็กทรอนิกส์ แบ่งได้เป็น

1. ข้อมูลทางคอมพิวเตอร์หรือข้อมูลทางอิเล็กทรอนิกส์ที่ได้จากการประมวลผลของเครื่องคอมพิวเตอร์หรือเครื่องอิเล็กทรอนิกส์ถือเป็นพยานหลักฐานโดยตรงซึ่งสามารถนำอ้างต่อศาลได้
2. ข้อมูลทางคอมพิวเตอร์หรือข้อมูลทางอิเล็กทรอนิกส์ที่ได้จากผลลัพธ์ของคอมพิวเตอร์หรือเป็นข้อมูลที่ทำซ้ำขึ้นถือเป็นพยานที่มีลักษณะเป็น Hearsay

โดยตามหลักกฎหมายว่าด้วยการรับฟังพยานหลักฐานของประเทศสหรัฐอเมริกาและประเทศสหราชอาณาจักรได้กำหนดให้เป็นข้อยกเว้นการห้ามรับฟังพยานหลักฐานที่มีลักษณะ Hearsay ทำให้พยานหลักฐานดังกล่าวสามารถรับฟังได้ ซึ่งกรณีนี้การปรับปรุงกฎหมายของไทยเกี่ยวกับพยานหลักฐานทางคอมพิวเตอร์หรือพยานหลักฐานทางอิเล็กทรอนิกส์อาจเปรียบเทียบจากแนวทางในการรับฟังพยานหลักฐานของประเทศสหรัฐอเมริกาและประเทศสหราชอาณาจักร โดยได้มีการศึกษาเป็นข้อพิจารณาและอธิบายไว้ในบทที่ 4 ดังที่ได้กล่าวมาแล้วข้างต้น

ทั้งนี้ผู้ศึกษาได้จัดทำตารางเปรียบเทียบมาตรการทางกฎหมายต่างๆ ที่บังคับใช้กับกระบวนการโอนเงินทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นมาตรการทางกฎหมายในการคุ้มครองผู้โอนภายใต้ระบบโอนเงินทางอิเล็กทรอนิกส์ หรือมาตรการในการกำหนดลักษณะความผิด รวมไปจนถึงมาตรการในการหยุดหรือระงับความเสียหายหรือเป็นบทลงโทษขั้นรุนแรงในมาตรการริบทรัพย์สินทั้งทางแพ่งและทางอาญา เพื่อเป็นข้อเสนอแนะและแนวทางเบื้องต้นในการปรับปรุงกฎหมายโอนเงินทางอิเล็กทรอนิกส์ของประเทศไทยต่อไป

เรื่อง	ประเทศสหรัฐอเมริกา (US)	ประเทศสหราชอาณาจักร (UK)	สหภาพยุโรป (EU)	องค์การสหประชาชาติ (UN)	ธนาคารระหว่างประเทศ	FATF	THAILAND
1.มาตรการทางกฎหมายในการป้องกันอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์							
1.1 การเปิดเผยข้อมูล ตามหลักการให้ลูกค้าแสดงตน	มี	มี	มี	มี	มี	มี	มี
1.2 การจัดทำบันทึกและรายงาน	มี	มี	มี	มี	มี	มี	มี
1.3 การให้ข้อมูลทางการเงินแก่หน่วยงานหรือเจ้าหน้าที่ของรัฐตามความจำเป็น	มี	มี	มี	ไม่มี	มี	มี	ไม่มี
1.4 มาตรการพิเศษเกี่ยวกับการฟอกเงิน	มี	มี	มี	มี	มี	มี	ไม่มี
1.5 กำหนดให้มีหน่วยงานหรือเจ้าหน้าที่เฉพาะในการตรวจสอบการโอนเงิน	มี	มี	มี	มี	มี	มี	ไม่มี
2.มาตรการในการกำหนดลักษณะความผิดและบทกำหนดโทษแก่อาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์							
2.1 ความผิดต่อการทุจริตต่อบัตร รหัส หรือสื่อทางอิเล็กทรอนิกส์	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี

หัวข้อ	ประเทศสหรัฐอเมริกา (US)	ประเทศสหราชอาณาจักร (UK)	สหภาพยุโรป (EU)	องค์การสหประชาชาติ (UN)	ธนาคารระหว่างประเทศ	FATF	THAILAND
2.2 ความผิดต่อการเข้าถึงบัตร รหัสหรือสื่อทางอิเล็กทรอนิกส์หรือฉ้อโกงบัตร	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี
2.3 ความผิดต่อการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี
2.4 ความผิดต่อการทุจริตโดยพนักงานหรือเจ้าหน้าที่ที่มีอำนาจหน้าที่ที่เกี่ยวข้องกับระบบการเงินการธนาคาร	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	มี
2.5 ความผิดต่อการฉ้อโกงธนาคาร	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	มี
2.6 ความผิดต่อการฟอกเงินทางการโอนเงินทางอิเล็กทรอนิกส์	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี
3.มาตรการทางกฎหมายในการแก้ไขเยียวยาความเสียหายที่เกิดขึ้นจากอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ (มาตรการริบทรัพย์สิน)	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี
4. มาตรการทางกฎหมายในการกำหนดหน่วยงานพิเศษเพื่อบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี

ศึกษาวิเคราะห์เปรียบเทียบมาตรการทางกฎหมายต่างประเทศที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์เพื่อเป็นแนวทางสำคัญของร่างกฎหมายโอนเงินทางอิเล็กทรอนิกส์ในการบังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ในประเทศไทย

ประเทศสหรัฐอเมริกา	ประเทศสหราชอาณาจักร	ประเทศไทย
พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 (Electronic Fund Transfers Act,1978) ตามมาตรา 1693 b และ มาตรา 1693 d	**พระราชบัญญัติธนาคารกลางแห่งสหราชอาณาจักร (Bank of England Act.1998) มาตรา 17**	<u>หลักเกณฑ์ในการโอนเงินทางอิเล็กทรอนิกส์</u> 1. ธนาคาร สถาบันทางการเงิน หรือนิติบุคคลที่ให้บริการทางการเงินการธนาคารรายอื่นๆ นอกเหนือจากธนาคารหรือสถาบันทางการเงินต้องมีการเปิดเผยข้อมูลในการโอนเงินทางอิเล็กทรอนิกส์แก่ผู้ใช้บริการ ซึ่งได้แก่ จำนวนเงิน ประเภทการโอน บัญชีธนาคารหรือบัญชีผู้โอน หรือผู้รับโอน ข้อมูลเฉพาะของบุคคลที่สาม
พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 (Electronic Fund Transfers Act, 1978) ตามมาตรา 1693c	**พระราชบัญญัติธนาคารกลางแห่งสหราชอาณาจักร (Bank of England Act.1998) ตามมาตรา 17.**	2. สถาบันทางการเงิน หรือธนาคารจะต้องจัดทำสรุปรายงานการเคลื่อนไหวทางบัญชีอิเล็กทรอนิกส์ หรือการเดินสะพัดแห่งบัญชีในการโอนเงินทางอิเล็กทรอนิกส์
พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 (Electronic Fund Transfers Act,1978)ตามมาตรา 1693 c ประกอบกับ พระราชบัญญัติความลับทางธนาคาร (Bank Secrecy Act)	**พระราชบัญญัติธนาคารกลางแห่งสหราชอาณาจักร (Bank of England Act,1998) ตามมาตรา 37.**	3. สถาบันทางการเงินหรือธนาคารอาจมีการเปิดเผยข้อมูลของผู้ใช้บริการในการโอนเงินทางอิเล็กทรอนิกส์ได้ในกรณีที่จำเป็นและเพื่อประโยชน์ในทางธุรกิจแก่บุคคลที่สาม หรือเพื่อประโยชน์แก่พนักงานเจ้าหน้าที่ซึ่งมีอำนาจหน้าที่ในการบังคับใช้กฎหมายตามกฎหมายที่บังคับใช้กับอาชญากรรมที่เกิดขึ้นในกระบวนการโอนเงินทางอิเล็กทรอนิกส์ภายใต้หลักการให้ลูกค้าแสดงตน หรือหลัก การแสดงข้อมูลเฉพาะบุคคลของลูกค้าของตน หรือ หลัก "khow your customer" เสมอ ซึ่งหลักการดังกล่าวประกอบด้วยการเปิดเผยข้อมูลดังต่อไปนี้ - ชื่อ นามสกุล - ที่อยู่ - อาชีพ - หนังสือเดินทาง - บัตรประกันสังคม

ประเทศสหรัฐอเมริกา	ประเทศสหราชอาณาจักร	ประเทศไทย
(ต่อ) พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 (Electronic Fund Transfers Act, 1978) มาตรา 1693 d	(ต่อ) พระราชบัญญัติธนาคารกลางแห่งสหราชอาณาจักร ค.ศ. 1998 (Bank of England Act,1998)	- ใบขับขี่รถยนต์ - หมายเลขประจำตัวผู้เสียภาษี - ข้อมูลอื่นๆ ที่เกี่ยวข้องกับที่มาของเงินดังกล่าว
พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 (Electronic Fund Transfers Act, 1978) มาตรา 1693 d ประกอบกับ พระราชบัญญัติความลับทางธนาคาร (Bank Secrecy Act)	พระราชบัญญัติธนาคารกลางแห่งสหราชอาณาจักร ค.ศ. 1998 (Bank of England Act,1998) ตามมาตรา 17	4. ผู้ใดเป็นผู้ใช้บริการในการโอนเงินทางอิเล็กทรอนิกส์ต้องเปิดเผยข้อมูลที่ถูกต้องของตนแก่ธนาคารหรือสถาบันทางการเงิน ไม่ว่าจะเป็นการแจ้งหมายเลขโทรศัพท์หรือที่อยู่ที่ถูกต้องของตนแก่ธนาคาร หรือสถาบันทางการเงิน ณ เวลาที่ทำการโอนเงินทางอิเล็กทรอนิกส์ดังกล่าว ทั้งนี้ การเปิดเผยข้อมูลการโอนเงินทาง อิเล็กทรอนิกส์ดังกล่าวต้องอยู่ภายใต้หลักการของ "know your customer" เสมอ
พระราชบัญญัติความลับทางธนาคาร (Bank Secrecy Act)	พระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceeds of Crime Act,2002)	5. ผู้ใดเป็นบุคคลหรือนิติบุคคลที่ทำการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งมีจำนวนเกินกว่า .....ขึ้นไป ต้องทำการรายงานธุรกรรมหรือความสัมพันธ์ที่มีต่อธนาคาร หรือสถาบันทางการเงิน โดยบุคคลหรือตัวแทนหรือผู้รับฝากเงินต้องรายงานการนำเงินหรือตราสารทางการเงินตามหลักเกณฑ์ที่รัฐมนตรีว่าการกระทรวงการคลังกำหนด
พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 (Electronic Fund Transfers Act,1978) ประกอบกับ พระราชบัญญัติความลับทางธนาคาร (Bank Secrecy Act) ประเทศสหรัฐอเมริกา	พระราชบัญญัติธนาคารกลางแห่งสหราชอาณาจักร (Bank of England Act.1998) มาตรา 38. ประกอบกับพระราชบัญญัติการดำเนินการกับ ประเทศสหราชอาณาจักร	<u>ความรับผิดทางอาญา</u> 1. ผู้ใดเพิกเฉย ละเลย หรือไม่ปฏิบัติตามหลักเกณฑ์เกี่ยวกับการเปิดเผยข้อมูลหรือการรายงานการโอนเงินทางอิเล็กทรอนิกส์ตามที่กล่าวมาแล้วข้างต้น หรือทำให้เกิดความล้มเหลวในการเปิดเผยข้อมูลหรือการรายงานการโอนเงินทางอิเล็กทรอนิกส์ หรือการแจ้งข้อความอันเป็นเท็จ หรือการแจ้งข้อความที่ไม่ตรงกับความจริงต่อการเปิดเผยข้อมูลหรือการรายงานการโอนเงินทางอิเล็กทรอนิกส์กรณีข้างต้น

		ประเทศไทย
(ต่อ) พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 (Electronic Fund Transfers Act,1978) ประกอบกับพระราชบัญญัติความลับทางธนาคาร (Bank Secrecy Act)	อาชญากรรม ค.ศ. 2002 (The Proceeds of Crime Act,2002)	ผู้ใดกระทำการข้างต้น ผู้นั้นมีความผิดและมีโทษปรับไม่เกิน.....บาท หรือมีโทษจำคุกไม่เกิน.....ปี หรือทั้งจำทั้งปรับ
พระราชบัญญัติโอนเงินทางอิเล็กทรอนิกส์ ค.ศ. 1978 (Electronic Fund Transfers Act,1978) มาตรา 1693 n (b) ประกอบกับประมวลกฎหมายอาญา (Federal Crime and Criminal Procedure) มาตรา 514.	พระราชบัญญัติการกระทำโดยมิชอบต่อคอมพิวเตอร์ (The Computer Misuse Act) ตามมาตรา 3	2. ผู้ใดกระทำการทุจริต ฉ้อโกง หลอกลวงต่อบัตรที่มีแถบแม่เหล็ก รหัสผ่าน หรือสื่อทางอิเล็กทรอนิกส์ หรือกระทำโดยทุจริต ฉ้อโกง หลอกลวงเพื่อให้ได้มาซึ่งบัตรที่มีแถบแม่เหล็ก รหัสผ่าน หรือสื่อทางอิเล็กทรอนิกส์ หรือใช้บัตรที่มีแถบแม่เหล็ก รหัสผ่านหรือสื่อทางอิเล็กทรอนิกส์โดยทุจริต โดยเจตนาให้มีผลต่อการโอนเงินทางอิเล็กทรอนิกส์ หรือเจตนาทุจริตเพื่อปกปิด หรือให้ได้มาซึ่งเงินของรัฐ หรือการกระทำทุจริตดังกล่าวซึ่งมีวัตถุประสงค์เพื่อให้มีการเปลี่ยนแปลงทางบัญชีในการโอนเงินทางอิเล็กทรอนิกส์ ผู้ใด กระทำการข้างต้น ผู้นั้นมีความผิดและมีโทษปรับไม่เกิน..... บาท หรือมีโทษจำคุกไม่เกิน.....ปี หรือทั้งจำทั้งปรับ
ประมวลกฎหมายอาญา (Federal Crime and Criminal Procedure) ว่าด้วยเรื่องการควบคุมการฉ้อโกงบัตรเครดิต ตามมาตรา 1029	พระราชบัญญัติการกระทำโดยมิชอบต่อคอมพิวเตอร์ (The Computer Misuse Act) ตามมาตรา 3	3. ผู้ใดซึ่ง สร้าง ใช้ สื่อสาร หรือส่งผ่านข้อมูลในการหลอกลวงการเข้าถึงเครื่องอิเล็กทรอนิกส์ในการโอนเงินทางอิเล็กทรอนิกส์โดยเจตนาฉ้อโกง 4. ผู้ใดซึ่ง สื่อสาร หรือการใช้ประโยชน์อย่างหนึ่งอย่างใดหรือมากกว่านั้น โดยเจตนาฉ้อโกงเพื่อการเข้าถึงเครื่องอิเล็กทรอนิกส์ในการโอนเงินโดยปราศจากอำนาจ 5. ผู้ใดซึ่ง ครอบงำอุปกรณ์อิเล็กทรอนิกส์ โดยเจตนาฉ้อโกง เพื่อหลอกลวงการเข้าถึงเครื่องอิเล็กทรอนิกส์ในการโอนเงินโดยปราศจาก

ประเทศสหรัฐอเมริกา	ประเทศสหราชอาณาจักร	ประเทศไทย
(ต่อ) ประมวลกฎหมายอาญา (Federal Crime and Criminal Procedure) ว่าด้วยเรื่องการควบคุมการฉ้อโกงบัตรเครดิต ตามมาตรา 1029	พระราชบัญญัติการกระทำโดยมิชอบต่อคอมพิวเตอร์ (The Computer Misuse Act) ตามมาตรา 3	อำนาจ 6. ผู้ใดซึ่ง สร้าง ส่งผ่านข้อมูลในการโอนเงินทางอิเล็กทรอนิกส์เพื่อการควบคุม เก็บรักษา ครอบงำอุปกรณ์อิเล็กทรอนิกส์ หรือการเข้าถึงเครื่องอิเล็กทรอนิกส์โดยเจตนาฉ้อโกง 7. ผู้ใดซึ่ง กระทำการอันมีผลกระทบต่อการเปลี่ยนแปลงทางบัญชีซึ่งมีผลต่อการเข้าถึงเครื่องอิเล็กทรอนิกส์ โดยเจตนาฉ้อโกงในการออกคำสั่งเพื่อให้ได้รับเงิน หรือสิ่งหนึ่งสิ่งใดจากคำสั่งดังกล่าว 8. ผู้ใดซึ่ง ออกคำสั่งเพื่อการเข้าถึงเครื่องเครื่องอิเล็กทรอนิกส์ หรือขายข้อมูลของเครื่องอิเล็กทรอนิกส์ ระบบคอมพิวเตอร์ เพื่อให้ได้มาซึ่งรหัส หรือมีการร้องขอใดๆ เพื่อการเข้าถึงข้อมูลทางอิเล็กทรอนิกส์โดยปราศจากอำนาจโดยมีวัตถุประสงค์ที่จะชักชวนบุคคลอื่นในการออกคำสั่งดังกล่าว ผู้ใดกระทำการข้างต้น ผู้นั้นมีความผิดและมีโทษปรับไม่เกิน.....บาท หรือมีโทษจำคุกไม่เกิน.....ปี หรือทั้งจำทั้งปรับ
ประมวลกฎหมายอาญา (Federal Crime and Criminal Procedure) ว่าด้วยเรื่องการควบคุมฉ้อโกงทางคอมพิวเตอร์ตามมาตรา 1030	พระราชบัญญัติการกระทำโดยมิชอบต่อคอมพิวเตอร์ (The Computer Misuse Act) ตามมาตรา 1 และ 2	9. ผู้ใดซึ่ง โดยเจตนาเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ หรือใช้อำนาจในการเข้าถึงคอมพิวเตอร์นั้นเพื่อการละเมิด หรือเพื่อให้ได้รับมาซึ่งข้อมูลทางบัญชีของธนาคาร ผู้ใดเจตนาฉ้อโกงการเข้าถึงระบบความปลอดภัยของคอมพิวเตอร์หรือระบบโอนเงินทางอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์ในการฉ้อโกงหรือให้ได้รับมาซึ่งประโยชน์อย่างหนึ่งอย่างใด 10. ผู้ใดเจตนาอันเป็นเหตุให้มีการส่งผ่านระบบข้อมูล รหัส หรือให้ได้มาซึ่งผลแห่งการกระทำใด ๆ อันก่อให้เกิดความเสียหายแก่ระบบความ

ประเทศสหรัฐอเมริกา	ประเทศสหราชอาณาจักร	ประเทศไทย
(ต่อ) ประมวลกฎหมายอาญา (Federal Crime and Criminal Procedure) ว่าด้วยเรื่องการควบคุมฉ้อโกงทางคอมพิวเตอร์ตามมาตรา 1030	(ต่อ) พระราชบัญญัติการกระทำโดยมิชอบต่อคอมพิวเตอร์ (The Computer Misuse Act) ตามมาตรา 1 และ 2	ปลอดภัยของคอมพิวเตอร์โดยปราศจากอำนาจและอาจสร้างความเสียหายให้แก่ระบบหรือคอมพิวเตอร์ภายใต้ระบบการโอนเงินทางอิเล็กทรอนิกส์ได้ ผู้ใด กระทำการข้างต้น ผู้นั้นมีความผิดและมีโทษปรับไม่เกิน..... บาท หรือมีโทษจำคุกไม่เกิน.....ปี หรือทั้งจำทั้งปรับ
ประมวลกฎหมายอาญา (Federal Crime and Criminal Procedure) ว่าด้วยพระราชบัญญัติควบคุมการฟอกเงิน (Money Laundering Control Act) ตามมาตรา 1956	พระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceeds of Crime Act,2002)	12. ผู้ใดโดยรู้ว่าเงิน หรือทรัพย์สินที่รวมอยู่ในการโอนเงินทางอิเล็กทรอนิกส์นั้นเป็นเงินหรือทรัพย์สินที่ได้มา หรือได้ประโยชน์ หรือใช้ในการกระทำอันเป็นความผิดทางอาญาอย่างหนึ่งอย่างใดๆ ตามกฎหมายนี้ และผู้นั้นจงใจหรือเจตนาปกปิด ปิดบังหรือเปลี่ยนแปลงที่มาที่แท้จริงของเงิน หรือทรัพย์สินดังกล่าว โดยการโอนเงินทางอิเล็กทรอนิกส์ ผู้ใด กระทำการข้างต้น ผู้นั้นมีความผิดและมีโทษปรับไม่เกิน.....บาท หรือมีโทษจำคุกไม่เกิน.....ปี หรือทั้งจำทั้งปรับ
ประมวลกฎหมายอาญา ว่าด้วยมาตรการริบทรัพย์สินทั้งการริบทรัพย์สินทางแพ่งตามมาตรา 981 และมาตรการริบทรัพย์สินทางอาญาตามมาตรา 982	พระราชบัญญัติการดำเนินการกับอาชญากรรม ค.ศ. 2002 (The Proceeds of Crime Act,2002) มาตรา 67	13 การกระทำใดๆ อันเป็นความผิดต่อการทุจริตหรือการฉ้อโกงต่อบัตรเครดิตหรือคอมพิวเตอร์ หรือกระทำความผิดใดๆ ต่อระบบหรือความปลอดภัยของโอนเงินทางอิเล็กทรอนิกส์ หรือความผิดฐานการโอนเงินทางอิเล็กทรอนิกส์เพื่อการฟอกเงินต้องดำเนินมาตรการริบทรัพย์สินทางแพ่ง ซึ่งเป็นมาตรการริบทรัพย์สินก่อนศาลมีคำพิพากษา หรือมาตรการริบทรัพย์สินทางอาญาซึ่งเป็นมาตรการริบทรัพย์สินหลังจากศาลมีคำพิพากษากรณีดังกล่าวแล้ว โดยมาตรการริบทรัพย์สินให้ดำเนินการยึดหรือริบเงินหรือทรัพย์สินทั้งหมดของผู้กระทำความผิด หากสืบเสาะได้ว่าทรัพย์สินดังกล่าวเป็นทรัพย์สินที่ได้มา หรือได้ประโยชน์ หรือใช้หรือเกี่ยวข้องกับการกระทำความผิดข้างต้น

รายการอ้างอิง

ภาษาไทย

เกียรติขจร วัจนะสวัสดิ์. คำอธิบายกฎหมายอาญาภาค 1. พิมพ์ครั้งที่ 3. กรุงเทพ : โรงพิมพ์มหาวิทยาลัยธรรมศาสตร์,2536

กองการประชุมสภา สภาผู้แทนราษฎร์. มติคณะรัฐมนตรีวันที่ 24 ธันวาคม2545 เรื่องพระราชบัญญัติแก้ไขเพิ่มเติมประมวลอาญา(ฉบับที่...) พ.ศ.....(กำหนดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์. ม.ป.ท :ม.ป.พ , 2545

การใช้เครื่องATM ของธนาคารพาณิชย์. ดอกเบี้ย(ธันวาคม 2527): 59-70

ก้องเกียรติ โอภาสวงการ,ดร. อิเลคโทรนิกส์แบงก์ คนยอมรับแค่ไหน. ดอกเบี้ย(กันยายน 2528): 134-142

ก้องเกียรติ โอภาสวงการ,ดร. โจรกรรมคอมพิวเตอร์ ตอน รหัสเอทีเอ็มเป็นเหตุ. ดอกเบี้ย (ธันวาคม 2528): 68-69

ก้องเกียรติ โอภาสวงการ,ดร. โจรกรรมคอมพิวเตอร์ ตอน ปล้นเอทีเอ็ม. ดอกเบี้ย(มกราคม 2529): 105-106

ก้องเกียรติ โอภาสวงการ,ดร. โจรกรรมคอมพิวเตอร์ ตอน เปิดประตูกลแล้วปล้นเงียบ. ดอกเบี้ย (พฤษภาคม 2529): 122-126

จรัสศรี จริยากูล. มาตรการทางกฎหมายเพื่อการป้องกันและปราบปรามอาชญากรรมบัตรเครดิต : วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์. บัณฑิตวิทยาลัย. จุฬาลงกรณ์มหาวิทยาลัย. , 2533

จักรรัตน์ ศรีโกมุท. อาชญากรรมทางเศรษฐกิจ : ศึกษากรณีอุปสรรคในการบังคับใช้กฎหมาย. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์. บัณฑิตวิทยาลัย. จุฬาลงกรณ์มหาวิทยาลัย. , 2539

จุลเจษฎ์ ฉัตราคม. พาณิชย์อิเล็กทรอนิกส์ อาชญากรรมคอมพิวเตอร์กับการพัฒนาการของสัญญาและกฎหมาย. ดุลพาห(พฤษภาคม-สิงหาคม 2543). 48(2): 12-20

จุมพล พันธุ์สัมฤทธิ์ อาชญากรรมทางเศรษฐกิจและมาตรการการแก้ไขในประเทศไทย. วารสารอัยการ.(เมษายน 2538): 65-89

ใจรัก เอื้อชูเกียรติ.ปัญหาทางกฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ : วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์. บัณฑิตวิทยาลัย.จุฬาลงกรณ์มหาวิทยาลัย ,2538

ชัยวัฒน์ วงศ์วัฒนศานต์ ; ทวีศักดิ์ กออนันตกูล ; สุรางคณา แก้วทนงค์. พระราชบัญญัติธุรกรรมอิเล็กทรอนิกส์.(ม.ป.ท.),2544.

ไชยยศ เหมะรัชตะ. เอกสารวิจัยส่วนบุคคล เรื่องมาตรการทางกฎหมายในการป้องกันและปราบปรามการฟอกเงิน. ม.ป.ป.

ไชยยศ เหมะรัชตะ. มาตรการทางกฎหมายในการป้องกันและปราบปรามการฟอกเงิน. วารสารราชบัณฑิตยสถาน(ตุลาคม 2541-มกราคม 2542). 24(1) : 28-42

ตร กวาดแก๊งฟอกเงิน. มติชน.(7 กันยายน 2544) :หน้า 1,28

เตรียมออกหมายเรียกฟอกเงิน 7 พันล้าน ระลอกสอง. มติชน (14 กันยายน 2544) : หน้า 32

ทวีศักดิ์ กออนันตกูล. อาชญากรรมในยุคโลกาภิวัฒน์. บทบัณฑิตย์(มีนาคม 2542): 26-39

ทักษินา จิรสิทธิ์. โจรกรรมคอมพิวเตอร์ระบาดนักคอมพิวเตอร์โกงเอทีเอ็มได้แนบเนียน. การเงินการธนาคาร.(มีนาคม 2530): 173-168

ธนาคารแห่งประเทศไทย. ระบบการชำระเงินในประเทศไทย กรุงเทพ : บริษัทประชุมทรงพริ้นติ้ง กรุ๊ป จำกัด, 2542

แนวคิดเรื่องกฎหมายการโอนเงินอิเล็กทรอนิกส์ จากการสัมมนาธนาคารแห่งประเทศไทย

ประไพพรรณ บุตรตัน. ความรับผิดเกี่ยวกับบัตรฝากและถอนเงินอัตโนมัติ: วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์. บัณฑิตวิทยาลัย.จุฬาลงกรณ์มหาวิทยาลัย, 2533

ปาริชาติ มุสิกะปาน. มาตรการในการป้องกันและปราบปรามการฟอกเงิน : ศึกษากรณีเทคโนโลยีสารสนเทศในเครือข่ายอินเตอร์เนตกับการฟอกเงิน. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาตร์ บัณฑิตวิทยาลัย.จุฬาลงกรณ์มหาวิทยาลัย, 2543

ปัญญา เปรมปรีดิ์,ดร. โจรกรรมด้วยเอทีเอ็ม. การเงินการธนาคาร(เมษายน 2529): 147-153

ปรพล สุกาวิล. กลลวงธุรกิจค้าเงินเถื่อน อันตรายยุคไอเอ็มเอฟ. สคบ สาร 21(222): 3-5

ปรียาลักษณ์ โทณะวณิก. ซื้อ ขาย แลก โอน เงินตราต่างประเทศ. จุลสาร กรุงเทพ ฉบับที่ 4/2527 : 1-59

พิชัย นิลทองคำ. ประมวลกฎหมายแพ่งและพาณิชย์ บรรพ 1-6 อาญา พิมพ์ครั้งที่ 2: อฑตยา

พิชัย นิลทองคำ. ประมวลกฎหมายวิธีพิจารณาความแพ่ง วิธีพิจารณาความอาญา พระธรรมนูญศาลยุติธรรม แก้ไขเพิ่มเติมปัจจุบัน VERSION 1.45

ภานุ รังสีสหัส. การกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์:วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาตร์ บัณฑิตวิทยาลัย.จุฬาลงกรณ์มหาวิทยาลัย, 2533

มโนช ตันตระเธียร,พ.ต.ต. ดร. อาชญากรรมในยุคโลกาภิวัฒน์จากการพนันบอลทางอินเตอร์เนทถึงอาชญากรรมคอมพิวเตอร์ ผู้ปฏิบัติในกระบวนการยุติธรรมไทยพร้อมหรือยัง ?. บทบัณฑิตย์(มีนาคม 2542) : 40-54

ยอดบัตรเอทีเอ็มพุ่งพรวด คนถือ 2 ล้าน 6 แสนใบ เผย 12 จุดอ่อนเอทีเอ็ม แบงค์ชาติออกโรงเตือนระวังโจรกรรมคอมพิวเตอร์. การเงินการธนาคาร(พฤษภาคม 2529) : 25-26

รณศักดิ์ เรืองวีรยุทธ์. ระบบการชำระเงินอิเล็กทรอนิกส์ของธนาคารแห่งประเทศไทย. ม.ป.ท: ม.ป.พ.,2545

เลิศชาย สุธรรมพร. อาชญากรรมคอมพิวเตอร์: ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล : วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ บัณฑิตวิทยาลัย.จุฬาลงกรณ์มหาวิทยาลัย. ,2541

วีระพงษ์ บุญโญภาส,รศ. อาชญากรรมทางเศรษฐกิจ. พิมพ์ครั้งที่ 3 กรุงเทพ : ห้างหุ้นส่วนจำกัด บี.เจ.เพลท โปรเซ็สเซอร์ ,2544

ศิระ บุญภินนท์. ความรับผิดทางอาญาของผู้ให้บริการอินเตอร์เนท ในการกระทำความผิดทางอาญาของผู่ใช้บริการ: ตัวอย่างจากสหรัฐอเมริกาและสหพันธสาธารณรัฐเยอรมัน. บทบัณฑิตย์ (มีนาคม 2542):68-88

ศูนย์ข้อมูลอาชญากรรมทางธุรกิจและการฟอกเงิน คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. งานสัมมนาทางวิชาการเรื่อง ระบบตรวจสอบการทุจริตในสถาบันการเงิน. ม.ป.ท. : ม.ป.พ. 2543

ศูนย์ข้อมูลอาชญากรรมทางธุรกิจและการฟอกเงิน คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. เอกสารประกอบการสัมมนาเรื่อง ประเทศไทยได้อะไรจากกฎหมายป้องกันและปราบปรามการฟอกเงิน. กรุงเทพ : ม.ป.พ. ,2541

สถาบันกฎหมายอาญา. รายงานสัมมนาทางวิชาการ โครงการ “ เวทีความคิดเพื่อการพัฒนากระบวนการยุติธรรมไทย” เรื่อง กฎหมายอาชญากรรมทางคอมพิวเตอร์ แนวทางในการแก้ไขปัญหาอาชญากรรมยุคไอที”. บทบัณฑิตย์(มีนาคม 2542): 156-215

สถาบันวิจัยเพื่อการพัฒนาประเทศไทย. ร่างรายงานการวิจัยฉบับสมบูรณ์ เรื่องนโยบายด้านอินเทอร์เน็ตสำหรับประเทศไทย.ม.ป.ท :ม.ป.พ, 2544

สถาบันฝึกอบรมและพัฒนาบุคลากร ธนาคารแห่งประเทศไทย.“การสัมมนาว่าด้วยการโอนเงินทางอิเล็กทรอนิกส์ ผ่านระบบการชำระเงิน. ม.ป.ท : ม.ป.พ, 2540

สังเกต ภู่กฤษณา.ความรับผิดของธนาคารเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ :วิทยานิพนธ์ปริญญามหาบัณฑิต. คณะนิติศาสตร์. บัณฑิตวิทยาลัย.มหาวิทยาลัยรามคำแหง., 2540

สีหนาท ประยูรรัตน์. คำอธิบายกฎหกระทรวง ระเบียบ และประกาศที่ออกตามความในพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2540 กรุงเทพ : ม.ป.พ. ,2542

สุเนติ คงเทพ. การไม่มีอำนาจเข้าสู่ระบบประมวลผล (Hacking). บทบัณฑิตย์(มีนาคม 2542) : 123-155

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ. ร่างพระราชว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ..... กรุงเทพ : หจก. จิรรัชการพิมพ์ ,2544

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ. รวมร่างกฎหมายเทคโนโลยีสารสนเทศภายใต้โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ. กรุงเทพ :โรงพิมพ์เดือนตุลา จำกัด, 2544

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ. รวมร่างกฎหมายเทคโนโลยีภายใต้โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ. พิมพ์ครั้งที่ 2.กรุงเทพ : เกสท์ ดีไซน์ แอนด์ พริ้นท์,2544

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ. โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ.พิมพ์ครั้งที่ 2. กรุงเทพ : โรงพิมพ์เดือนตุลา จำกัด, 2544

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ.บันทึกหลักการและเหตุผลประกอบร่างพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ....(ม.ป.ท:ม.ป.พ), 2541

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ.บันทึกหลักการและเหตุผลประกอบร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์(ฉบับผ่านความเห็นชอบของคณะกรรมการเทคโนโลยีแห่งชาติ เมื่อวันที่ 2 พฤษภาคม 2545) ม.ป.ท.: ม.ป.พ, 2545

สำนักงานป้องกันและปราบปรามการฟอกเงิน. รวมกฎหมายป้องกันและปราบปรามการฟอกเงิน พระราชบัญญัติ พระราชกฤษฎีกา กฎกระทรวง ระเบียบและประกาศที่เกี่ยวข้อง. ม.ป.ท.: ม.ป.พ, 2544

สมเกียรติ์ ตั้งกิจวาณิชย์.รายงานการวิจัยเรื่อง ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง. ม.ป.ท.:ม.ป.พ, 2542

เอกสารประกอบการสัมมนาเรื่อง “กฎหมายเกี่ยวกับพาณิชย์อิเล็กทรอนิกส์ Electronic Commerce Law”, 2543

เอกสารประกอบการสัมมนาเรื่อง “กฎหมายการพัฒนาโครงสร้างพัฒนาสารสนเทศให้ทั่วถึงและเท่าเทียมกัน” ม.ป.ท.:ม.ป.พ, 2544

อนุชิต อนุชิตานุกูล; สมเกียรติ์ ตั้งกิจวาณิชย์.รายงานการวิจัยฉบับสมบูรณ์ เงินอิเล็กทรอนิกส์กับนโยบายการเงินและการฟอกเงิน. ม.ป.ท.:ม.ป.พ, 2543

อำนาจ เนตยสุภา. ภาษาอังกฤษสำหรับนักกฎหมาย. ข่าวเนติบัณฑิตยสภา(สิงหาคม 2545) 15 (157): 14-15

อัมพร ณ ตะกั่วทุ่ง,บรรณาธิการ. รวมคำบรรยาย : ภาคหนึ่ง สมัยที่ 43 ปีการศึกษา 2533 เล่มที่ 17 กรุงเทพ: บริษัท กรุงสยาม พริ้นติ้ง กรุ๊ป จำกัด, 2533

ภาษาอังกฤษ

A Report of The President' s Working Group on Unlawful Conduct on The Internet. The electronic Frontier : The Challenge of Unlawful Conduct Involving The Use of The Internet. [online] Available from :http://www.usdoj.gov/criminal/cybercrime.[4/06/2002]

Computer Crime And Intellectual Property Section (CCIP) :Searching And Seizing Computers And Obtaining Electronic Evidence in Criminal Investigations. [online] Available from : http://www.usdoj.gov/criminal/cybercrime/searchmanual.html [5/032003]

Computer Crime And Intellectual Property Section (CCIP) :Federal Computer Intrusion Laws. [online] Available from : http://www.usdoj.gov/criminal/cybercrime/cclaws.html[5/032003]

Computer Crime And Intellectual Property Section (CCIP) :Computer Intrusion cases. [online] Available from : http://www.usdoj.gov/ccclaws.html[5/032003]

Computer Crime And Intellectual Property Section (CCIP):Field Guidance on New Authorities That Relate to Computer Crime And Electronic Evidence Enacted in The USA patriot Act of 2001. [online] Available from : http://www.cybercrime.gov/PatriotAct.htm[5/032003]

Council of Europe. Convention on Crime. [online] Available from : http://www.conventions.coe.int[4/06/2002]

Crime in Cyberspace First Draft of International Convention Release For Public Discussion. [online] Available from http://www.politechbot.com/docs/treaty.html [5/03/2003]

Deak, Nicholas L. ;Celusak ,Joanne. International Banking . NEWYORK (1984)

Decision of The European Central Bank of 7 October 1999 on Fraud Prevention (ECB/1999/5). [online] Available from : http://www.europa.ru.int/eur-lex/en/lif/dat/1999/en_399DO726.html[4/08/2002]

Department of Justice. [online] Available from : http://www.usdoj.gov/criminal/cybercrime. [10/01/2003]

Directive 2000/46/ECOF The European Parliament And of The Council of 18 September 2000 on the Taking Up, Pursuit of And Prudential Supervision of The Business

Of Electronic Money Institution. [online] Available from : http://europa.eu.int[04/08/2002]

EFTA COURT [online] Available from:http://www.efta.int/docs/court/information/intro.htm [04/08/2002]

European Central Bank Regulation(EC) NO 2157/1999 of 23 September 1999 on THE Powers of The European Central Bank to Inpose Sanctions(ECB/1999/4). [online] Available from : http://europa.eu.int/eur-lex/en/lif/dat/1999/en_399R2157.html[04/08/2002]

Explanatory Report of Convention on Laundering, Search, Seizure And Confiscation of the proceeds From Crime (ETS no.141). [online] Available from : http://www.conventions.coe.int[18/06/2002]

Explanatory Report of Convention on Laundering, Search, Seizure And Confiscation of the proceeds From Crime (ETS no.185)adopted on 8 November 2001. [online] Available from : http://www.conventions.coe.int[18/06/2002]

Electronic Discovery And Computer Forensics Case List. [online] Available from : http://www.krollontrack.com[05/03/2003]

European Working Party on Information Technology Crime. [online] Available from : http://www.interpol.int/technologycrime/woekingparties/default.asp[05/03/2003]

Federal Rules of Criminal Procedure. Effective March 21, 1946 as Amended to December 1, 1998. [online] Available from http://www.law.gov.au/ecommerce [04/04/2002]

Financial Crime [online] Available from http://www.Interpol.int/public/financialcrime/default.asp [06/08/2003]

International Criminal Law Association(ICLA). [online] Available from : http://www.jus.uio.no[06/08/2003]

Lectric Law Library ‘s Stacks. Electronic Fund Transfers. [online] Available from : http://www.lectlaw.com/files/ban13.htm[17/09/2002]

Molander, RogerC. ; Mussington ,David A. ; Wilson, Peter A. Cyberpayments And Money Laundering Problems and Promise. WASHINGTON D.C. :RAND

Smedinghoff , Thomas J. Online Law The SPA’S Legal Guide to Doing Business on The Internet. CANADA :N.P.

Stabla ,Witold Electronic Payment System Criminal [online] Available from : http://www.epaymentsystem.eu[08/05/2002]

The Law of Electronic Fund Transfers [online] Available from : http://caselaw.lp.findlaw.com[15/06/2002]

The U.S. Government Printing Office Via GPO Access. Code of Federal Regulations Title 12 : Bank And Banking, Chapter 2: Federal Reserve System , Part 200 TO 219 (Revise as of January 1 ,2001) [online] Available from : http://caselaw.lp.findlaw.com. [06/08/2002]

Vartanian ,Thomas P. ;Ledig ,Robert H. ;Bruneau Lynn. 21ST Century Money,Banking&Commmerce. N.D.

U.S. Department of Justice. Russian Computer Hacker Sentenced to Three Years in Prison . [online] Available from : http://cybercrime. Gov/gorshkovSent.htm.[05/04/2003]

U.S. Department of Justice. Two Kazakhstan Citizens Accused of Breaking Into Bloomberg L.P.'S Computer fraud Extortion Are Extradited. [online] Available from : http://cybercrime.Gov/blloombergindict.html.[05/04/2003]

United Nations Commission on international Trade Law (UNCITRAL). UNCITRAL Model Law on International Credit Transfers. [online] Available from : http://www.uncitral.org/English/texts/payments/ml-credittrans.htm [07/05/2002]

United State Code : Title 15: Consumer Credit Protection. Chapter 41 : Consumer Credit Protection Subchapter 6 : Electronic Fund Transfer. [online] Available from : http://caselaw.lp.findlaw.com.,[05/06/2002]

United State Code : Title 18 : Crime And Criminal Procedure. [online] Available from : http://caselaw.lp.findlaw.com.[05/06/2002]

United State Code : Title 31: Money And Finance. [online] Available from : http://caselaw.lp.findlaw.com[05/06/2002]

ภาคผนวก

Electronic Fund Transfer Act

Sec. 1693. - Congressional findings and declaration of purpose

(a) Rights and liabilities undefined

The Congress finds that the use of electronic systems to transfer funds provides the potential for substantial benefits to consumers. However, due to the unique characteristics of such systems, the application of existing consumer protection legislation is unclear, leaving the rights and liabilities of consumers, financial institutions, and intermediaries in electronic fund transfers undefined.

(b) Purposes

It is the purpose of this subchapter to provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems. The primary objective of this subchapter, however, is the provision of individual consumer rights

Sec. 1693a. - Definitions

As used in this subchapter -

(1)

the term ''accepted card or other means of access'' means a card, code, or other means of access to a consumer's account for the purpose of initiating electronic fund transfers when the person to whom such card or other means of access was issued has requested and received or has signed or has used, or authorized another to use, such card or other means of access for the purpose of transferring money between accounts or obtaining money, property, labor, or services;

(2)

the term ''account'' means a demand deposit, savings deposit, or other asset account (other than an occasional or incidental credit balance in an open end credit plan as defined in section 1602(i) of this title), as described in regulations of the Board, established primarily for personal, family, or household purposes, but such term does not include an account held by a financial institution pursuant to a bona fide trust agreement;

(3)

the term ''Board'' means the Board of Governors of the Federal Reserve System;

(4)

the term ''business day'' means any day on which the offices of the consumer's financial institution involved in an electronic fund transfer are open to the public for carrying on substantially all of its business functions;

(5)

the term ''consumer'' means a natural person;

(6)

the term ''electronic fund transfer'' means any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account. Such term includes, but is not limited to, point-of-sale transfers, automated teller machine transactions, direct deposits or withdrawals of funds, and transfers initiated by telephone. Such term does not include -

(A)

any check guarantee or authorization service which does not directly result in a debit or credit to a consumer's account:

(B)

any transfer of funds, other than those processed by automated clearinghouse, made by a financial institution on behalf of a consumer by means of a service that transfers funds held at either Federal Reserve banks or other depository institutions and which is not designed primarily to transfer funds on behalf of a consumer;

(C)

any transaction the primary purpose of which is the purchase or sale of securities or commodities through a broker-dealer registered with or regulated by the Securities and Exchange Commission;

(D)

any automatic transfer from a savings account to a demand deposit account pursuant to an agreement between a consumer and a financial institution for the purpose of covering an overdraft or maintaining an agreed upon minimum balance in the consumer's demand deposit account; or

(E)

any transfer of funds which is initiated by a telephone conversation between a consumer and an officer or employee of a financial institution which is not pursuant to a prearranged

plan and under which periodic or recurring transfers are not contemplated;

as determined under regulations of the Board;

(7)

the term ''electronic terminal'' means an electronic device, other than a telephone operated by a consumer, through which a consumer may initiate an electronic fund transfer. Such term includes, but is not limited to, point-of-sale terminals, automated teller machines, and cash dispensing machines;

(8)

the term ''financial institution'' means a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person who, directly or indirectly, holds an account belonging to a consumer;

(9)

the term ''preauthorized electronic fund transfer'' means an electronic fund transfer authorized in advance to recur at substantially regular intervals;

(10)

the term ''State'' means any State, territory, or possession of the United States, the District of Columbia, the Commonwealth of Puerto Rico, or any political subdivision of any of the foregoing; and

(11)

the term ''unauthorized electronic fund transfer'' means an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit, but the term does not include any electronic fund transfer

(A)

initiated by a person other than the consumer who was furnished with the card, code, or other means of access to such consumer's account by such consumer, unless the consumer has notified the financial institution involved that transfers by such other person are no longer authorized,

(B)

initiated with fraudulent intent by the consumer or any person acting in concert with the consumer, or

(C)

which constitutes an error committed by a financial institution

Sec. 1693b. - Regulations

(a) Prescription by Board

The Board shall prescribe regulations to carry out the purposes of this subchapter. In prescribing such regulations, the Board shall:

(1)

consult with the other agencies referred to in section 1693o of this title and take into account, and allow for, the continuing evolution of electronic banking services and the technology utilized in such services,

(2)

prepare an analysis of economic impact which considers the costs and benefits to financial institutions, consumers, and other users of electronic fund transfers, including the extent to which additional documentation, reports, records, or other paper work would be required, and the effects upon competition in the provision of electronic banking services among large and small financial institutions and the availability of such services to different classes of consumers, particularly low income consumers,

(3)

to the extent practicable, the Board shall demonstrate that the consumer protections of the proposed regulations outweigh the compliance costs imposed upon consumers and financial institutions, and

(4)

any proposed regulations and accompanying analyses shall be sent promptly to Congress by the Board.

(b) Issuance of model clauses

The Board shall issue model clauses for optional use by financial institutions to facilitate compliance with the disclosure requirements of section 1693c of this title and to aid consumers in understanding the rights and responsibilities of participants in electronic fund transfers by utilizing readily understandable language. Such model clauses shall be adopted after notice duly given in the Federal Register and opportunity for public comment in accordance with section 553 of title 5. With respect to the disclosures required by section 1693c(a)(3) and (4) of this title, the Board

shall take account of variations in the services and charges under different electronic fund transfer systems and, as appropriate, shall issue alternative model clauses for disclosure of these differing account terms.

(c) Criteria; modification of requirements

Regulations prescribed hereunder may contain such classifications, differentiations, or other provisions, and may provide for such adjustments and exceptions for any class of electronic fund transfers, as in the judgment of the Board are necessary or proper to effectuate the purposes of this subchapter, to prevent circumvention or evasion thereof, or to facilitate compliance therewith. The Board shall by regulation modify the requirements imposed by this subchapter on small financial institutions if the Board determines that such modifications are necessary to alleviate any undue compliance burden on small financial institutions and such modifications are consistent with the purpose and objective of this subchapter.

(d) Applicability to service providers other than certain financial institutions

(1) In general

If electronic fund transfer services are made available to consumers by a person other than a financial institution holding a consumer's account, the Board shall by regulation assure that the disclosures, protections, responsibilities, and remedies created by this subchapter are made applicable to such persons and services.

(2) State and local government electronic benefit transfer systems

(A) ''Electronic benefit transfer system'' defined

In this paragraph, the term ''electronic benefit transfer system'' -

(i)

means a system under which a government agency distributes needs-tested benefits by establishing accounts that may be accessed by recipients electronically, such as through automated teller machines or point-of-sale terminals; and

(ii)

does not include employment-related payments, including salaries and pension, retirement, or unemployment benefits established by a Federal, State, or local government agency.

(B) Exemption generally

The disclosures, protections, responsibilities, and remedies established under this subchapter, and any regulation prescribed or order issued by the Board in accordance with this subchapter, shall not apply to any electronic benefit transfer system established under State or local law or administered by a State or local government.

(C) Exception for direct deposit into recipient's account

Subparagraph (B) shall not apply with respect to any electronic funds transfer under an electronic benefit transfer system for a deposit directly into a consumer account held by the recipient of the benefit.

(D) Rule of construction

No provision of this paragraph -

(i)

affects or alters the protections otherwise applicable with respect to benefits established by any other provision [1] Federal, State, or local law; or ''of''.

(ii)

otherwise supersedes the application of any State or local law.

(3) Fee disclosures at automated teller machines

(A) In general

The regulations prescribed under paragraph (1) shall require any automated teller machine operator who imposes a fee on any consumer for providing host transfer services to such consumer to provide notice in accordance with subparagraph (B) to the consumer (at the time the service is provided) of -

(i)

the fact that a fee is imposed by such operator for providing the service; and

(ii)

the amount of any such fee.

(B) Notice requirements

(i) On the machine

The notice required under clause (i) of subparagraph (A) with respect to any fee described in such subparagraph shall be posted in a prominent and conspicuous location on or at the automated teller machine at which the electronic fund transfer is initiated by the consumer.

(ii) On the screen

The notice required under clauses (i) and (ii) of subparagraph (A) with respect to any fee described in such subparagraph shall appear on the screen of the automated teller machine, or on a paper notice issued from such machine, after the transaction is initiated and before the consumer is irrevocably committed to completing the transaction, except that during the period beginning on November 12, 1999, and ending on December 31, 2004, this clause shall not apply to any automated teller machine that lacks the technical capability to disclose the notice on the screen or to issue a paper notice after the transaction is initiated and before the consumer is irrevocably committed to completing the transaction.

(C) Prohibition on fees not properly disclosed and explicitly assumed by consumer

No fee may be imposed by any automated teller machine operator in connection with any electronic fund transfer initiated by a consumer for which a notice is required under subparagraph (A), unless -

(i)

the consumer receives such notice in accordance with subparagraph (B); and

(ii)

the consumer elects to continue in the manner necessary to effect the transaction after receiving such notice.

(D) Definitions

For purposes of this paragraph, the following definitions shall apply:

(i) Automated teller machine operator

The term ''automated teller machine operator'' means any person who -

(I)

operates an automated teller machine at which consumers initiate electronic fund transfers; and

(II)

is not the financial institution that holds the account of such consumer from which the transfer is made.

(ii) Electronic fund transfer

The term ''electronic fund transfer'' includes a transaction that involves a balance inquiry initiated by a consumer in the same manner as an electronic fund transfer, whether or not the consumer initiates a transfer of funds in the course of the transaction.

(iii) Host transfer services

The term ''host transfer services'' means any electronic fund transfer made by an automated teller machine operator in connection with a transaction initiated by a consumer at an automated teller machine operated by such operator

Sec. 1693c. - Terms and conditions of transfers

(a) Disclosures; time; form; contents

The terms and conditions of electronic fund transfers involving a consumer's account shall be disclosed at the time the consumer contracts for an electronic fund transfer service, in accordance with regulations of the Board. Such disclosures shall be in readily understandable language and shall include, to the extent applicable -

(1)

the consumer's liability for unauthorized electronic fund transfers and, at the financial institution's option, notice of the advisability of prompt reporting of any loss, theft, or unauthorized use of a card, code, or other means of access;

(2)

the telephone number and address of the person or office to be notified in the event the consumer believes than [1] an unauthorized electronic fund transfer has been or may be effected;

(3)

the type and nature of electronic fund transfers which the consumer may initiate, including any limitations on the frequency or

dollar amount of such transfers, except that the details of such limitations need not be disclosed if their confidentiality is necessary to maintain the security of an electronic fund transfer system, as determined by the Board;

(4)

any charges for electronic fund transfers or for the right to make such transfers;

(5)

the consumer's right to stop payment of a preauthorized electronic fund transfer and the procedure to initiate such a stop payment order;

(6)

the consumer's right to receive documentation of electronic fund transfers under section 1693d of this title;

(7)

a summary, in a form prescribed by regulations of the Board, of the error resolution provisions of section 1693f of this title and the consumer's rights thereunder. The financial institution shall thereafter transmit such summary at least once per calendar year;

(8)

the financial institution's liability to the consumer under section 1693h of this title;

(9)

under what circumstances the financial institution will in the ordinary course of business disclose information concerning the consumer's account to third persons; and

(10)

a notice to the consumer that a fee may be imposed by -

(A)

an automated teller machine operator (as defined in section 1693b(d)(3)(D)(i) of this title) if the consumer initiates a transfer from an automated teller machine that is not operated by the person issuing the card or other means of access; and

(B)

any national, regional, or local network utilized to effect the transaction.

(b) Notification of changes to consumer

A financial institution shall notify a consumer in writing at least twenty-one days prior to the effective date of any change in any term or condition of the consumer's account required to be disclosed under subsection (a) of this section if such change would result in greater cost or liability for such consumer or decreased access to the consumer's account. A financial institution may, however, implement a change in the terms or conditions of an account without prior notice when such change is immediately necessary to maintain or restore the security of an electronic fund transfer system or a consumer's account. Subject to subsection (a)(3) of this section, the Board shall require subsequent notification if such a change is made permanent.

(c) Time for disclosures respecting accounts accessible prior to effective date of this subchapter

For any account of a consumer made accessible to electronic fund transfers prior to the effective date of this subchapter, the information required to be disclosed to the consumer under subsection (a) of this section shall be disclosed not later than the earlier of -

(1)

the first periodic statement required by section 1693d(c) of this title after the effective date of this subchapter; or

(2)

thirty days after the effective date of this subchapter

Sec. 1693d. - Documentation of transfers

(a) Availability of written documentation to consumer; contents

For each electronic fund transfer initiated by a consumer from an electronic terminal, the financial institution holding such consumer's account shall, directly or indirectly, at the time the transfer is initiated, make available to the consumer written documentation of such transfer. The documentation shall clearly set forth to the extent applicable -

(1)

the amount involved and date the transfer is initiated;

(2)

the type of transfer;

(3)

the identity of the consumer's account with the financial institution from which or to which funds are transferred;

(4)

the identity of any third party to whom or from whom funds are transferred; and

(5)

the location or identification of the electronic terminal involved.

(b) Notice of credit to consumer

For a consumer's account which is scheduled to be credited by a preauthorized electronic fund transfer from the same payor at least once in each successive sixty-day period, except where the payor provides positive notice of the transfer to the consumer, the financial institution shall elect to provide promptly either positive notice to the consumer when the credit is made as scheduled, or negative notice to the consumer when the credit is not made as scheduled, in accordance with regulations of the Board. The means of notice elected shall be disclosed to the consumer in accordance with section 1693c of this title.

(c) Periodic statement; contents

A financial institution shall provide each consumer with a periodic statement for each account of such consumer that may be accessed by means of an electronic fund transfer. Except as provided in subsections (d) and (e) of this section, such statement shall be provided at least monthly for each monthly or shorter cycle in which an electronic fund transfer affecting the account has occurred, or every three months, whichever is more frequent. The statement, which may include information regarding transactions other than electronic fund transfers, shall clearly set forth -

(1)

with regard to each electronic fund transfer during the period, the information described in subsection (a) of this section, which may be provided on an accompanying document;

(2)

the amount of any fee or charge assessed by the financial institution during the period for electronic fund transfers or for account maintenance;

(3)

the balances in the consumer's account at the beginning of the period and at the close of the period; and

(4)

the address and telephone number to be used by the financial institution for the purpose of receiving any statement inquiry or notice of account error from the consumer. Such address and telephone number shall be preceded by the caption ''Direct Inquiries To:'' or other similar language indicating that the address and number are to be used for such inquiries or notices.

(d) Consumer passbook accounts

In the case of a consumer's passbook account which may not be accessed by electronic fund transfers other than preauthorized electronic fund transfers crediting the account, a financial institution may, in lieu of complying with the requirements of subsection (c) of this section, upon presentation of the passbook provide the consumer in writing with the amount and date of each such transfer involving the account since the passbook was last presented.

(e) Accounts other than passbook accounts

In the case of a consumer's account, other than a passbook account, which may not be accessed by electronic fund transfers other than preauthorized electronic fund transfers crediting the account, the financial institution may provide a periodic statement on a quarterly basis which otherwise complies with the requirements of subsection (c) of this section.

(f) Documentation as evidence

In any action involving a consumer, any documentation required by this section to be given to the consumer which indicates that an electronic fund transfer was made to another person shall be admissible as evidence of such transfer and shall constitute prima facie proof that such transfer was made

Sec. 1693e. - Preauthorized transfers

(a)

A preauthorized electronic fund transfer from a consumer's account may be authorized by the consumer only in writing, and a copy of such authorization shall be provided to the consumer when made. A consumer may stop payment of a preauthorized electronic fund transfer by notifying the financial institution orally or in writing at any time up to three business days preceding the scheduled date of such transfer. The financial institution may require written confirmation to be provided to it within fourteen days of an oral notification if, when the oral notification is made, the consumer is

advised of such requirement and the address to which such confirmation should be sent.

(b)

In the case of preauthorized transfers from a consumer's account to the same person which may vary in amount, the financial institution or designated payee shall, prior to each transfer, provide reasonable advance notice to the consumer, in accordance with regulations of the Board, of the amount to be transferred and the scheduled date of the transfer

Sec. 1693f. - Error resolution

(a) Notification to financial institution of error

If a financial institution, within sixty days after having transmitted to a consumer documentation pursuant to section 1693d(a), (c), or (d) of this title or notification pursuant to section 1693d(b) of this title, receives oral or written notice in which the consumer -

(1)

sets forth or otherwise enables the financial institution to identify the name and account number of the consumer;

(2)

indicates the consumer's belief that the documentation, or, in the case of notification pursuant to section 1693d(b) of this title, the consumer's account, contains an error and the amount of such error; and

(3)

sets forth the reasons for the consumer's belief (where applicable) that an error has occurred,

the financial institution shall investigate the alleged error, determine whether an error has occurred, and report or mail the results of such investigation and determination to the consumer within ten business days. The financial institution may require written confirmation to be provided to it within ten business days of an oral notification of error if, when the oral notification is made, the consumer is advised of such requirement and the address to which such confirmation should be sent. A financial institution which requires written confirmation in accordance with the previous sentence need not provisionally recredit a consumer's account in accordance with subsection (c) of this section, nor shall the financial institution be liable under subsection (e) of this section if the written confirmation is not received within the ten-day period referred to in the previous sentence.

Electronic Fund Transfer Act

(b) Correction of error; interest

If the financial institution determines that an error did occur, it shall promptly, but in no event more than one business day after such determination, correct the error, subject to section 1693g of this title, including the crediting of interest where applicable.

(c) Provisional recredit of consumer's account

If a financial institution receives notice of an error in the manner and within the time period specified in subsection (a) of this section, it may, in lieu of the requirements of subsections (a) and (b) of this section, within ten business days after receiving such notice provisionally recredit the consumer's account for the amount alleged to be in error, subject to section 1693g of this title, including interest where applicable, pending the conclusion of its investigation and its determination of whether an error has occurred. Such investigation shall be concluded not later than forty-five days after receipt of notice of the error. During the pendency of the investigation, the consumer shall have full use of the funds provisionally recredited.

(d) Absence of error; finding; explanation

If the financial institution determines after its investigation pursuant to subsection (a) or (c) of this section that an error did not occur, it shall deliver or mail to the consumer an explanation of its findings within 3 business days after the conclusion of its investigation, and upon request of the consumer promptly deliver or mail to the consumer reproductions of all documents which the financial institution relied on to conclude that such error did not occur. The financial institution shall include notice of the right to request reproductions with the explanation of its findings.

(e)

Treble damages If in any action under section 1693m of this title, the court finds that -

(1)

the financial institution did not provisionally recredit a consumer's account within the ten-day period specified in subsection (c) of this section, and the financial institution

(A)

did not make a good faith investigation of the alleged error, or

(B)

did not have a reasonable basis for believing that the consumer's account was not in error; or

Electronic Fund Transfer Act

(2)

the financial institution knowingly and willfully concluded that the consumer's account was not in error when such conclusion could not reasonably have been drawn from the evidence available to the financial institution at the time of its investigation,

then the consumer shall be entitled to treble damages determined under section 1693m(a)(1) of this title.

(f) Acts constituting error

For the purpose of this section, an error consists of -

(1)

an unauthorized electronic fund transfer;

(2)

an incorrect electronic fund transfer from or to the consumer's account;

(3)

the omission from a periodic statement of an electronic fund transfer affecting the consumer's account which should have been included;

(4)

a computational error by the financial institution;

(5)

the consumer's receipt of an incorrect amount of money from an electronic terminal;

(6)

a consumer's request for additional information or clarification concerning an electronic fund transfer or any documentation required by this subchapter; or

(7)

any other error described in regulations of the Board

Electronic Fund Transfer Act

Sec. 1693g. - Consumer liability

(a) Unauthorized electronic fund transfers; limit

A consumer shall be liable for any unauthorized electronic fund transfer involving the account of such consumer only if the card or other means of access utilized for such transfer was an accepted card or other meanas [1] of access and if the issuer of such card, code, or other means of access has provided a means whereby the user of such card, code, or other means of access can be identified as the person authorized to use it, such as by signature, photograph, or fingerprint or by electronic or mechanical confirmation. In no event, however, shall a consumer's liability for an unauthorized transfer exceed the lesser of -

(1)

$50; or

(2)

the amount of money or value of property or services obtained in such unauthorized electronic fund transfer prior to the time the financial institution is notified of, or otherwise becomes aware of, circumstances which lead to the reasonable belief that an unauthorized electronic fund transfer involving the consumer's account has been or may be effected. Notice under this paragraph is sufficient when such steps have been taken as may be reasonably required in the ordinary course of business to provide the financial institution with the pertinent information, whether or not any particular officer, employee, or agent of the financial institution does in fact receive such information.

Notwithstanding the foregoing, reimbursement need not be made to the consumer for losses the financial institution establishes would not have occurred but for the failure of the consumer to report within sixty days of transmittal of the statement (or in extenuating circumstances such as extended travel or hospitalization, within a reasonable time under the circumstances) any unauthorized electronic fund transfer or account error which appears on the periodic statement provided to the consumer under section 1693d of this title. In addition, reimbursement need not be made to the consumer for losses which the financial institution establishes would not have occurred but for the failure of the consumer to report any loss or theft of a card or other means of access within two business days after the consumer learns of the loss or theft (or in extenuating circumstances such as extended travel or hospitalization, within a longer period which is reasonable under the circumstances), but the consumer's liability under this subsection in any such case may not exceed a total of $500, or the amount of unauthorized electronic fund transfers which occur following the close of two business days (or such longer period) after the consumer learns of the loss or theft but prior to notice to the financial institution under this subsection, whichever is less.

(b) Burden of proof

Electronic Fund Transfer Act

In any action which involves a consumer's liability for an unauthorized electronic fund transfer, the burden of proof is upon the financial institution to show that the electronic fund transfer was authorized or, if the electronic fund transfer was unauthorized, then the burden of proof is upon the financial institution to establish that the conditions of liability set forth in subsection (a) of this section have been met, and, if the transfer was initiated after the effective date of section 1693c of this title, that the disclosures required to be made to the consumer under section 1693c(a)(1) and (2) of this title were in fact made in accordance with such section.

(c) Determination of limitation on liability

In the event of a transaction which involves both an unauthorized electronic fund transfer and an extension of credit as defined in section 1602(e) of this title pursuant to an agreement between the consumer and the financial institution to extend such credit to the consumer in the event the consumer's account is overdrawn, the limitation on the consumer's liability for such transaction shall be determined solely in accordance with this section.

(d) Restriction on liability

Nothing in this section imposes liability upon a consumer for an unauthorized electronic fund transfer in excess of his liability for such a transfer under other applicable law or under any agreement with the consumer's financial institution.

(e) Scope of liability

Except as provided in this section, a consumer incurs no liability from an unauthorized electronic fund transfer

Sec. 1693h. - Liability of financial institutions

(a) Action or failure to act proximately causing damages

Subject to subsections (b) and (c) of this section, a financial institution shall be liable to a consumer for all damages proximately caused by -

(1)

the financial institution's failure to make an electronic fund transfer, in accordance with the terms and conditions of an account, in the correct amount or in a timely manner when properly instructed to do so by the consumer, except where -

(A)

the consumer's account has insufficient funds;

(B)

the funds are subject to legal process or other encumbrance restricting such transfer;

(C)

such transfer would exceed an established credit limit;

(D)

an electronic terminal has insufficient cash to complete the transaction; or

(E)

as otherwise provided in regulations of the Board;

(2)

the financial institution's failure to make an electronic fund transfer due to insufficient funds when the financal [1] institution failed to credit, in accordance with the terms and conditions of an account, a deposit of funds to the consumer's account which would have provided sufficient funds to make the transfer, and

(3)

the financial institution's failure to stop payment of a preauthorized transfer from a consumer's account when instructed to do so in accordance with the terms and conditions of the account.

(b) Acts of God and technical malfunctions

A financial institution shall not be liable under subsection (a)(1) or (2) of this section if the financial institution shows by a preponderance of the evidence that its action or failure to act resulted from -

(1)

an act of God or other circumstance beyond its control, that it exercised reasonable care to prevent such an occurrence, and that it exercised such diligence as the circumstances required; or

(2)

a technical malfunction which was known to the consumer at the time he attempted to initiate an electronic fund transfer or, in the case of a preauthorized transfer, at the time such transfer should have occurred.

(c) Intent

In the case of a failure described in subsection (a) of this section which was not intentional and which resulted from a bona fide error, notwithstanding the maintenance of procedures reasonably adapted to avoid any such error, the financial institution shall be liable for actual damages proved.

(d) Exception for damaged notices

If the notice required to be posted pursuant to section 1693b(d)(3)(B)(i) of this title by an automated teller machine operator has been posted by such operator in compliance with such section and the notice is subsequently removed, damaged, or altered by any person other than the operator of the automated teller machine, the operator shall have no liability under this section for failure to comply with section 1693b(d)(3)(B)(i) of this title

Sec. 1693i. - Issuance of cards or other means of access

(a) Prohibition; proper issuance

No person may issue to a consumer any card, code, or other means of access to such consumer's account for the purpose of initiating an electronic fund transfer other than -

(1)

in response to a request or application therefor; or

(2)

as a renewal of, or in substitution for, an accepted card, code, or other means of access, whether issued by the initial issuer or a successor.

(b) Exceptions

Notwithstanding the provisions of subsection (a) of this section, a person may distribute to a consumer on an unsolicited basis a card, code, or other means of access for use in initiating an electronic fund transfer from such consumer's account, if -

(1)

such card, code, or other means of access is not validated;

(2)

such distribution is accompanied by a complete disclosure, in accordance with section 1693c of this title, of the consumer's rights and liabilities which will apply if such card, code, or other means of access is validated;

(3)

such distribution is accompanied by a clear explanation, in accordance with regulations of the Board, that such card, code, or other means of access is not validated and how the consumer may dispose of such code, card, or other means of access if validation is not desired; and

(4)

such card, code, or other means of access is validated only in response to a request or application from the consumer, upon verification of the consumer's identity.

(c) Validation

For the purpose of subsection (b) of this section, a card, code, or other means of access is validated when it may be used to initiate an electronic fund transfer

Sec. 1693j. - Suspension of obligations

If a system malfunction prevents the effectuation of an electronic fund transfer initiated by a consumer to another person, and such other person has agreed to accept payment by such means, the consumer's obligation to the other person shall be suspended until the malfunction is corrected and the electronic fund transfer may be completed, unless such other person has subsequently, by written request, demanded payment by means other than an electronic fund transfer

Sec. 1693k. - Compulsory use of electronic fund transfers

No person may -

(1)

condition the extension of credit to a consumer on such consumer's repayment by means of preauthorized electronic fund transfers; or

(2)

require a consumer to establish an account for receipt of electronic fund transfers with a particular financial institution as a condition of employment or receipt of a government benefit

Electronic Fund Transfer Act

Sec. 1693l. - Waiver of rights

No writing or other agreement between a consumer and any other person may contain any provision which constitutes a waiver of any right conferred or cause of action created by this subchapter. Nothing in this section prohibits, however, any writing or other agreement which grants to a consumer a more extensive right or remedy or greater protection than contained in this subchapter or a waiver given in settlement of a dispute or action

Sec. 1693m. - Civil liability

(a) Individual or class action for damages; amount of award

Except as otherwise provided by this section and section 1693h of this title, any person who fails to comply with any provision of this subchapter with respect to any consumer, except for an error resolved in accordance with section 1693f of this title, is liable to such consumer in an amount equal to the sum of -

(1)

any actual damage sustained by such consumer as a result of such failure;

(2)

(A)

in the case of an individual action, an amount not less than $100 nor greater than $1,000; or

(B)

in the case of a class action, such amount as the court may allow, except that

(i)

as to each member of the class no minimum recovery shall be applicable, and

(ii)

the total recovery under this subparagraph in any class action or series of class actions arising out of the same failure to comply by the same person shall not be more than the lesser of $500,000 or 1 per centum of the net worth of the defendant; and

(3)

in the case of any successful action to enforce the foregoing liability, the costs of the action, together with a reasonable attorney's fee as determined by the court.

(b) Factors determining amount of award

In determining the amount of liability in any action under subsection (a) of this section, the court shall consider, among other relevant factors -

(1)

in any individual action under subsection (a)(2)(A) of this section, the frequency and persistence of noncompliance, the nature of such noncompliance, and the extent to which the noncompliance was intentional; or

(2)

in any class action under subsection (a)(2)(B) of this section, the frequency and persistence of noncompliance, the nature of such noncompliance, the resources of the defendant, the number of persons adversely affected, and the extent to which the noncompliance was intentional.

(c) Unintentional violations; bona fide error

Except as provided in section 1693h of this title, a person may not be held liable in any action brought under this section for a violation of this subchapter if the person shows by a preponderance of evidence that the violation was not intentional and resulted from a bona fide error notwithstanding the maintenance of procedures reasonably adapted to avoid any such error.

(d) Good faith compliance with rule, regulation, or interpretation of Board or approval of duly authorized official or employee of Federal Reserve System

Federal Reserve System

No provision of this section or section 1693n of this title imposing any liability shall apply to -

(1)

any act done or omitted in good faith in conformity with any rule, regulation, or interpretation thereof by the Board or in conformity with any interpretation or approval by an official or employee of the Federal Reserve System duly authorized by the Board to issue such interpretations or approvals under such procedures as the Board may prescribe therefor; or

Electronic Fund Transfer Act

(2)

any failure to make disclosure in proper form if a financial institution utilized an appropriate model clause issued by the Board,

notwithstanding that after such act, omission, or failure has occurred, such rule, regulation, approval, or model clause is amended, rescinded, or determined by judicial or other authority to be invalid for any reason.

(e) Notification to consumer prior to action; adjustment of consumer's account

A person has no liability under this section for any failure to comply with any requirement under this subchapter if, prior to the institution of an action under this section, the person notifies the consumer concerned of the failure, complies with the requirements of this subchapter, and makes an appropriate adjustment to the consumer's account and pays actual damages or, where applicable, damages in accordance with section 1693h of this title.

(f) Action in bad faith or for harassment; attorney's fees

On a finding by the court that an unsuccessful action under this section was brought in bad faith or for purposes of harassment, the court shall award to the defendant attorney's fees reasonable in relation to the work expended and costs.

(g) Jurisdiction of courts; time for maintenance of action

Without regard to the amount in controversy, any action under this section may be brought in any United States district court, or in any other court of competent jurisdiction, within one year from the date of the occurrence of the violation

Sec. 1693n. - Criminal liability

(a) Violations respecting giving of false or inaccurate information, failure to provide information, and failure to comply with provisions of this subchapter

Whoever knowingly and willfully -

(1)

gives false or inaccurate information or fails to provide information which he is required to disclose by this subchapter or any regulation issued thereunder; or

(2)

otherwise fails to comply with any provision of this subchapter;

shall be fined not more than $5,000 or imprisoned not more than one year, or both.

(b) Violations affecting interstate or foreign commerce

Whoever -

(1)

knowingly, in a transaction affecting interstate or foreign commerce, uses or attempts or conspires to use any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument to obtain money, goods, services, or anything else of value which within any one-year period has a value aggregating $1,000 or more; or

(2)

with unlawful or fraudulent intent, transports or attempts or conspires to transport in interstate or foreign commerce a counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument knowing the same to be counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained; or

(3)

with unlawful or fraudulent intent, uses any instrumentality of interstate or foreign commerce to sell or transport a counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument knowing the same to be counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained; or

(4)

knowingly receives, conceals, uses, or transports money, goods, services, or anything else of value (except tickets for interstate or foreign transportation) which

(A)

within any one-year period has a value aggregating $1,000 or more,

(B)

has moved in or is part of, or which constitutes interstate or foreign commerce, and

(C)

has been obtained with a counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument; or

(5)

knowingly receives, conceals, uses, sells, or transports in interstate or foreign commerce one or more tickets for interstate or foreign transportation, which

(A)

within any one-year period have a value aggregating $500 or more, and

(B)

have been purchased or obtained with one or more counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument; or

(6)

in a transaction affecting interstate or foreign commerce, furnishes money, property, services, or anything else of value, which within any one-year period has a value aggregating $1,000 or more, through the use of any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument knowing the same to be counterfeit, fictitious, altered, forged, lost, stolen,or fraudulently obtained - shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(c) ''Debit instrument'' defined

As used in this section, the term ''debit instrument'' means a card, code, or other device, other than a check, draft, or similar paper instrument, by the use of which a person may initiate an electronic fund transfer

Sec. 1693o. - Administrative enforcement

(a) Enforcing agencies

Compliance with the requirements imposed under this subchapter shall be enforced under -

(1)

section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of -

(A)

national banks, and Federal branches and Federal agencies of foreign banks, by the Office of the Comptroller of the Currency;

(B)

member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25(a) [1] of the Federal Reserve Act (12 U.S.C. 601 et seq., 611 et seq.), by the Board; and

(C)

banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System) and insured State branches of foreign banks, by the Board of Directors of the Federal Deposit Insurance Corporation;

(2)

section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), by the Director of the Office of Thrift Supervision, in the case of a savings association the deposits of which are insured by the Federal Deposit Insurance Corporation;

(3)

the Federal Credit Union Act (12 U.S.C. 1751 et seq.), by the Administrator of the National Credit Union Administration with respect to any Federal credit union. [2]

(4)

part A of subtitle VII of title 49, by the Secretary of Transportation, with respect to any air carrier or foreign air carrier subject to that part; and

(5)

the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.), by the Securities and Exchange Commission, with respect to any broker or dealer subject to that Act.

The terms used in paragraph (1) that are not defined in this subchapter or otherwise defined in section 3(s) of the Federal Deposit Insurance Act (12 U.S.C. 1813(s)) shall have the meaning given to them in section 1(b) of the International Banking Act of 1978 (12 U.S.C. 3101).

(b) Violations of subchapter deemed violations of pre-existing statutory requirements; additional powers

For the purpose of the exercise by any agency referred to in subsection (a) of this section of its powers under any Act referred to in that subsection, a violation of any requirement imposed under this subchapter shall be deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in subsection (a) of this section, each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this subchapter, any other authority conferred on it by law.

(c) Overall enforcement authority of Federal Trade Commission

Except to the extent that enforcement of the requirements imposed under this subchapter is specifically committed to some other Government agency under subsection (a) of this section, the Federal Trade Commission shall enforce such requirements. For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act (15 U.S.C. 41 et seq.), a violation of any requirement imposed under this subchapter shall be deemed a violation of a requirement imposed under that Act. All of the functions and powers of the Federal Trade Commission under the Federal Trade Commission Act are available to the Commission to enforce compliance by any person subject to the jurisdiction of the Commission with the requirements imposed under this subchapter, irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act

Sec. 1693p. - Reports to Congress

(a)

Not later than twelve months after the effective date of this subchapter and at one-year intervals thereafter, the Board shall make reports to the Congress concerning the administration of its functions under this subchapter, including such recommendations as the Board deems necessary and appropriate. In addition, each report of the Board shall include its assessment of the extent to which compliance with this subchapter is being achieved, and a summary of the enforcement actions taken under section 1693o of this title. In such report, the Board shall particularly address the effects of this subchapter on the costs and benefits to financial institutions and consumers, on competition, on the introduction of new technology, on the operations of financial institutions, and on the adequacy of consumer protection.

(b)

In the exercise of its functions under this subchapter, the Board may obtain upon request the views of any other Federal agency which, in the judgment of the Board, exercises regulatory or supervisory functions with respect to any class of persons subject to this subchapt

Electronic Fund Transfer Act

Sec. 1693q. - Relation to State laws

This subchapter does not annul, alter, or affect the laws of any State relating to electronic fund transfers, except to the extent that those laws are inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency. A State law is not inconsistent with this subchapter if the protection such law affords any consumer is greater than the protection afforded by this subchapter. The Board shall, upon its own motion or upon the request of any financial institution, State, or other interested party, submitted in accordance with procedures prescribed in regulations of the Board, determine whether a State requirement is inconsistent or affords greater protection. If the Board determines that a State requirement is inconsistent, financial institutions shall incur no liability under the law of that State for a good faith failure to comply with that law, notwithstanding that such determination is subsequently amended, rescinded, or determined by judicial or other authority to be invalid for any reason. This subchapter does not extend the applicability of any such law to any class of persons or transactions to which it would not otherwise apply

Sec. 215. - Receipt of commissions or gifts for procuring loans

(a)

Whoever -

(1)

corruptly gives, offers, or promises anything of value to any person, with intent to influence or reward an officer, director, employee, agent, or attorney of a financial institution in connection with any business or transaction of such institution; or

(2)

as an officer, director, employee, agent, or attorney of a financial institution, corruptly solicits or demands for the benefit of any person, or corruptly accepts or agrees to accept, anything of value from any person, intending to be influenced or rewarded in connection with any business or transaction of such institution;

shall be fined not more than $1,000,000 or three times the value of the thing given, offered, promised, solicited, demanded, accepted, or agreed to be accepted, whichever is greater, or imprisoned not more than 30 years, or both, but if the value of the thing given, offered, promised, solicited, demanded, accepted, or agreed to be accepted does not exceed $1,000, shall be fined under this title or imprisoned not more than one year, or both.

(b)

Transferred)

(c)

This section shall not apply to bona fide salary, wages, fees, or other compensation paid, or expenses paid or reimbursed, in the usual course of business.

(d)

Federal agencies with responsibility for regulating a financial institution shall jointly establish such guidelines as are appropriate to assist an officer, director, employee, agent, or attorney of a financial institution to comply with this section. Such agencies shall make such guidelines available to the public

TITLE 18 > PART I > CHAPTER 31 > Sec. 655.

Prev | Next

Sec. 655. - Theft by bank examiner

Whoever, being a bank examiner or assistant examiner, steals, or unlawfully takes, or unlawfully conceals any money, note, draft, bond, or security or any other property of value in the possession of any bank or banking institution which is a member of the Federal Reserve System, which is insured by the Federal Deposit Insurance Corporation, which is a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978), or which is an organization operating under section 25 or section 25(a) [1] of the Federal Reserve Act, or from any safe deposit box in or adjacent to the premises of such bank, branch, agency, or organization, shall be fined under this title or imprisoned not more than five years, or both; but if the amount taken or concealed does not exceed $1,000, he shall be fined under this title or imprisoned not more than one year, or both; and shall be disqualified from holding office as a national bank examiner or Federal Deposit Insurance Corporation examiner.

This section shall apply to all public examiners and assistant examiners who examine member banks of the Federal Reserve System, banks the deposits of which are insured by the Federal Deposit Insurance Corporation, branches or agencies of foreign banks (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978), or organizations operating under section 25 or section 25(a) [1] of the Federal Reserve Act, whether appointed by the Comptroller of the Currency, by

Federal Deposit Insurance Corporation, or appointed or elected under the laws of any State; but shall not apply to private examiners or assistant examiners employed only by a clearing-house association or by the directors of a bank

---

TITLE 18 > PART I > CHAPTER 31 > Sec. 656.

Prev | Next

Sec. 656. - Theft, embezzlement, or misapplication by bank officer or employee

Whoever, being an officer, director, agent or employee of, or connected in any capacity with any Federal Reserve bank, member bank, depository institution holding company, national bank, insured bank, branch or agency of a foreign bank, or organization operating under section 25 or section 25(a) [1] of the Federal Reserve Act, or a receiver of a national bank, insured bank, branch, agency, or organization or any agent or employee of the receiver, or a Federal Reserve Agent, or an agent or employee of a Federal Reserve Agent or of the Board of Governors of the Federal Reserve System, embezzles, abstracts, purloins or willfully misapplies any of the moneys, funds or credits of such bank, branch, agency, or organization or holding company or any moneys, funds, assets or securities intrusted to the custody or care of such bank, branch, agency, or organization, or holding company or to the custody or care of any such agent, officer, director, employee or receiver, shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both; but if the amount embezzled, abstracted, purloined or misapplied does not exceed $1,000, he shall be fined under this title or imprisoned not more than one year, or both.

As used in this section, the term ''national bank'' is synonymous with ''national banking association''; ''member bank'' means and includes any national bank, state bank, or bank and trust company which has become a member of one of the Federal Reserve banks; ''insured bank'' includes any

the Federal Deposit Insurance Corporation; and the term ''branch or agency of a foreign bank'' means a branch or agency described in section 20(9) of this title. For purposes of this section, the term ''depository institution holding company'' has the meaning given such term in section 3 of the Federal Deposit Insurance Act

Sec. 657. - Lending, credit and insurance institutions

Whoever, being an officer, agent or employee of or connected in any capacity with the Federal Deposit Insurance Corporation, National Credit Union Administration, Office of Thrift Supervision, the Resolution Trust Corporation, any Federal home loan bank, the Federal Housing Finance Board, Farm Credit Administration, Department of Housing and Urban Development, Federal Crop Insurance Corporation, the Secretary of Agriculture acting through the Farmers Home Administration or successor agency, the Rural Development Administration or successor agency, or the Farm Credit System Insurance Corporation, a Farm Credit Bank, a bank for cooperatives or any lending, mortgage, insurance, credit or savings and loan corporation or association authorized or acting under the laws of the United States or any institution, other than an insured bank (as defined in section 656), the accounts of which are insured by the Federal Deposit Insurance Corporation, or by the National Credit Union Administration Board or any small business investment company, or any community development financial institution receiving financial assistance under the Riegle Community Development and Regulatory Improvement Act of 1994, and whoever, being a receiver of any such institution, or agent or employee of the receiver, embezzles, abstracts, purloins or willfully misapplies any moneys, funds, credits, securities or other things of value belonging to such institution, or pledged or otherwise intrusted to its care, shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both; but if the amount or value embezzled, abstracted, purloined or misapplied does not exceed $1,000, he shall be fined under this title or imprisoned not more than one year, or both

TITLE 18 > PART I > CHAPTER 31 > Sec. 666.

Prev | Next

Sec. 666. - Theft or bribery concerning programs receiving Federal funds

(a)

Whoever, if the circumstance described in subsection (b) of this section exists -

(1)

being an agent of an organization, or of a State, local, or Indian tribal government, or any agency thereof -

(A)

embezzles, steals, obtains by fraud, or otherwise without authority knowingly converts to the use of any person other than the rightful owner or intentionally misapplies, property that -

(i)

is valued at $5,000 or more, and

(ii)

is owned by, or is under the care, custody, or control of such organization, government, or agency; or

(B)

corruptly solicits or demands for the benefit of any person, or accepts or agrees to accept, anything of value from any person, intending to be influenced or rewarded in connection with any business, transaction, or series of transactions of such organization, government, or agency involving any thing of value of $5,000 or more; or

(2)

corruptly gives, offers, or agrees to give anything of value to any person, with intent to influence or reward an agent of an organization or of a State, local or Indian tribal government, or any agency thereof, in connection with any business, transaction, or series of transactions of such organization, government, or agency involving anything of value of $5,000 or more;

shall be fined under this title, imprisoned not more than 10 years, or both.

(b)

The circumstance referred to in subsection (a) of this section is that the organization, government, or agency receives, in any one year period, benefits in excess of $10,000 under a Federal program involving a grant, contract, subsidy, loan, guarantee, insurance, or other form of Federal assistance.

(c)

This section does not apply to bona fide salary, wages, fees, or other compensation paid, or expenses paid or reimbursed, in the usual course of business.

(d)

As used in this section -

(1)

the term ''agent'' means a person authorized to act on behalf of another person or a government and, in the case of an organization or government, includes a servant or employee, and a partner, director, officer, manager, and representative;

(2)

the term ''government agency'' means a subdivision of the executive, legislative, judicial, or other branch of government, including a department, independent establishment, commission, administration, authority, board, and bureau, and a corporation or other legal entity established, and subject to control, by a government or governments for the execution of a governmental or intergovernmental program;

(3)

the term ''local'' means of or pertaining to a political subdivision within a State;

(4)

the term ''State'' includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States; and

(5)

the term ''in any one-year period'' means a continuous period that commences no earlier than twelve months before the commission of the offense or that ends no later than twelve months after the commission of the offense. Such period may include time both before and after the commission of the offense

TITLE 18 > PART I > CHAPTER 47 > Sec. 1005.

Sec. 1005. - Bank entries, reports and transactions

Whoever, being an officer, director, agent or employee of any Federal Reserve bank, member bank, depository institution holding company, national bank, insured bank, branch or agency of a foreign bank, or organization operating under section 25 or section 25(a) [1] of the Federal Reserve Act,, (FOOTNOTE 2) without authority from the directors of such bank, branch, agency, or organization or company, issues or puts in circulation any notes of such bank, branch, agency, or organization or company; or [2] So in original.

Whoever, without such authority, makes, draws, issues, puts forth, or assigns any certificate of deposit, draft, order, bill of exchange, acceptance, note, debenture, bond, or other obligation, or mortgage, judgment or decree; or

Whoever makes any false entry in any book, report, or statement of such bank, company, branch, agency, or organization with intent to injure or defraud such bank, company, branch, agency, or organization, or any other company, body politic or corporate, or any individual person, or to

Insurance Corporation, or any agent or examiner appointed to examine the affairs of such bank, company, branch, agency, or organization, or the Board of Governors of the Federal Reserve System; [3] ''or''.

Whoever with intent to defraud the United States or any agency thereof, or any financial institution referred to in this section, participates or shares in or receives (directly or indirectly) any money, profit, property, or benefits through any transaction, loan, commission, contract, or any other act of any such financial institution - Shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

As used in this section, the term ''national bank'' is synonymous with ''national banking association''; ''member bank'' means and includes any national bank, state bank, or bank or trust company, which has become a member of one of the Federal Reserve banks; ''insured bank'' includes any state bank, banking association, trust company, savings bank, or other banking institution, the deposits of which are insured by the Federal Deposit Insurance Corporation; and the term ''branch or agency of a foreign bank'' means a branch or agency described in section 20(9) of this title. For purposes of this section, the term ''depository institution holding company'' has the meaning given such term in section 3(w)(1) of the Federal Deposit Insurance Act

---

TITLE 18 > PART I > CHAPTER 47 > Sec. 1006.

Prev | Next

Sec. 1006. - Federal credit institution entries, reports and transactions

Whoever, being an officer, agent or employee of or connected in any capacity with the Federal Deposit Insurance Corporation, National Credit Union Administration, Office of Thrift Supervision, any Federal home loan bank, the Federal Housing Finance Board, the Resolution Trust Corporation, Farm Credit Administration, Department of Housing and Urban Development, Federal Crop Insurance Corporation, the Secretary of Agriculture acting through the Farmers Home Administration or successor agency, the Rural Development

cooperatives or any lending, mortgage, insurance, credit or savings and loan corporation or association authorized or acting under the laws of the United States or any institution, other than an insured bank (as defined in section 656), the accounts of which are insured by the Federal Deposit Insurance Corporation, or by the National Credit Union Administration Board or any small business investment company, with intent to defraud any such institution or any other company, body politic or corporate, or any individual, or to deceive any officer, auditor, examiner or agent of any such institution or of department or agency of the United States, makes any false entry in any book, report or statement of or to any such institution, or without being duly authorized, draws any order or bill of exchange, makes any acceptance, or issues, puts forth or assigns any note, debenture, bond or other obligation, or draft, bill of exchange, mortgage, judgment, or decree, or, with intent to defraud the United States or any agency thereof, or any corporation, institution, or association referred to in this section, participates or shares in or receives directly or indirectly any money, profit, property, or benefits through any transaction, loan, commission, contract, or any other act of any such corporation, institution, or association, shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both

TITLE 18 > PART I > CHAPTER 47 > Sec. 1007.

Prev | Next

Sec. 1007. - Federal Deposit Insurance Corporation transactions

Whoever, for the purpose of influencing in any way the action of the Federal Deposit Insurance Corporation, knowingly makes or invites reliance on a false, forged, or counterfeit statement, document, or thing shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both

TITLE 18 > PART I > CHAPTER 63 > Sec. 1344.

Prev | Next

Sec. 1344. - Bank fraud

Whoever knowingly executes, or attempts to execute, a scheme or artifice -

(1)

to defraud a financial institution; or

(2)

to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises;

shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both

TITLE 18 > PART I > CHAPTER 25 > Sec. 513.

Sec. 513. - Securities of the States and private entities

(a)

Whoever makes, utters or possesses a counterfeited security of a State or a political subdivision thereof or of an organization, or whoever makes, utters or possesses a forged security of a State or political subdivision thereof or of an organization, with intent to deceive another person, organization, or government shall be fined under this title [1] or imprisoned for not more than ten years, or both.

(b)

Whoever makes, receives, possesses, sells or otherwise transfers an implement designed for or particularly suited for making a counterfeit or forged security with the intent that it be so used shall be punished by a fine under this title or by imprisonment for not more than ten years, or both.

(c)

For purposes of this section -

(1)

the term ''counterfeited'' means a document that purports to be genuine but is not, because it has been falsely made or manufactured in its entirety;

(2)

the term ''forged'' means a document that purports to be genuine but is not because it has been falsely altered, completed, signed, or endorsed, or contains a false addition thereto or insertion therein, or is a combination of parts of two or more genuine documents;

(3)

the term ''security'' means -

(A)

a note, stock certificate, treasury stock certificate, bond, treasury bond, debenture, certificate of deposit, interest coupon, bill, check, draft, warrant, debit instrument as defined in section 916(c) of the Electronic Fund Transfer Act, money order, traveler's check, letter of credit, warehouse receipt, negotiable bill of lading, evidence of indebtedness, certificate of interest in or participation in any profit-sharing agreement, collateral-trust certificate, pre-reorganization certificate of subscription, transferable share, investment contract, voting trust certificate, or certificate of interest in tangible or intangible property;

(B)

an instrument evidencing ownership of goods, wares, or merchandise;

(C)

security;

(D)

a certificate of interest in, certificate of participation in, certificate for, receipt for, or warrant or option or other right to subscribe to or purchase, any of the foregoing; or

(E)

a blank form of any of the foregoing;

(4)

the term ''organization'' means a legal entity, other than a government, established or organized for any purpose, and includes a corporation, company, association, firm, partnership, joint stock company, foundation, institution, society, union, or any other association of persons which operates in or the activities of which affect interstate or foreign commerce; and

(5)

the term ''State'' includes a State of the United States, the District of Columbia, Puerto Rico, Guam, the Virgin Islands, and any other territory or possession of the United States

TITLE 18 > PART I > CHAPTER 47 > Sec. 1029.

Prev | Next

Sec. 1029. - Fraud and related activity in connection with access devices

(a)

Whoever -

(1)

devices;

(2)

knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3)

knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4)

knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(5)

knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6)

without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of -

(A)

offering an access device; or

(B)

selling information regarding or an application to obtain an access device;

(7)

possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8)

knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9)

knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10)

without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device;

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b)

(1)

Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.

(2)

Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section

under subsection (c) of this section, or both.

(c) Penalties. -

(1) Generally. -

The punishment for an offense under subsection (a) of this section is -

(A)

in the case of an offense that does not occur after a conviction for another offense under this section -

(i)

if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

(ii)

if the offense is under paragraph (4), (5), (8), or (9), [1] of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

(B)

in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

(C)

in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

(2) Forfeiture procedure. -

The forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial proceeding, shall be governed by section 413 of the Controlled Substances Act, except for subsection (d) of that section.

(d)

The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e)

As used in this section -

(1)

the term ''access device'' means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

(2)

the term ''counterfeit access device'' means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

(3)

the term ''unauthorized access device'' means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;

(4)

the term ''produce'' includes design, alter, authenticate, duplicate, or assemble;

(5)

the term ''traffic'' means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of;

(6)

the term ''device-making equipment'' means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device;

(7)

the term ''credit card system member'' means a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system;

(8)

the term ''scanning receiver'' means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument [2]

(9)

the term ''telecommunications service'' has the meaning given such term in section 3 of title I of the Communications Act of 1934 (47 U.S.C. 153);

(10)

the term ''facilities-based carrier'' means an entity that owns communications transmission facilities, is responsible for the operation and maintenance of those facilities, and holds an operating license issued by the Federal Communications Commission under the authority of title III of the Communications Act of 1934; and

(11)

the term ''telecommunication identifying information'' means electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument.

(f)

enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title. For purposes of this subsection, the term ''State'' includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(g)

(1)

It is not a violation of subsection (a)(9) for an officer, employee, or agent of, or a person engaged in business with, a facilities-based carrier, to engage in conduct (other than trafficking) otherwise prohibited by that subsection for the purpose of protecting the property or legal rights of that carrier, unless such conduct is for the purpose of obtaining telecommunications service provided by another facilities-based carrier without the authorization of such carrier.

(2)

In a prosecution for a violation of subsection (a)(9), (other than a violation consisting of producing or trafficking) it is an affirmative defense (which the defendant must establish by a preponderance of the evidence) that the conduct charged was engaged in for research or development in connection with a lawful purpose.

(h)

Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if -

(1)

the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within the jurisdiction of the United States; and

(2)

the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom

---

TITLE 18 > PART I > CHAPTER 47 > Sec. 1030.

Prev | Next

Sec. 1030. - Fraud and related activity in connection with computers

(a)

Whoever -

(1)

having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2)

intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A)

information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B)

information from any department or agency of the United States; or

(C)

information from any protected computer if the conduct involved an interstate or foreign communication;

(3)

intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4)

knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

(A)

(i)

knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii)

intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii)

intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B)

by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused) -

(i)

loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii)

the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii)

physical injury to any person;

(iv)

a threat to public health or safety; or

(v)

damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6)

knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if -

(A)

such trafficking affects interstate or foreign commerce; or

(B)

such computer is used by or for the Government of the United States; [1] ''or''.

(7)

with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b)

Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c)

The punishment for an offense under subsection (a) or (b) of this section is -

(1)

(A)

a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B)

a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A)

except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B)

a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if -

(i)

the offense was committed for purposes of commercial advantage or private financial gain;

(ii)

Constitution or laws of the United States or of any State; or

(iii)

the value of the information obtained exceeds $5,000; [2] So in original. Probably should be followed by ''and''.

(C)

a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A)

a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B)

a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) [3] (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(4)

(A)

a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B)

a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C)

a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.

(d)

(1)

The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2)

The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3)

Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e)

As used in this section -

(1)

the term ''computer'' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2)

the term ''protected computer'' means a computer -

(A)

exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B)

which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3)

the term ''State'' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4)

the term ''financial institution'' means -

(A)

an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B)

the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C)

a credit union with accounts insured by the National Credit Union Administration;

(D)

a member of the Federal home loan bank system and any home loan bank;

(E)

any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F)

a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G)

the Securities Investor Protection Corporation;

(H)

a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I)

an organization operating under section 25 or section 25(a) [4] of the Federal Reserve Act. (FOOTNOTE 5) [5] So in original. The period probably should be a semicolon.

(5)

the term ''financial record'' means information

institution;

(6)

the term ''exceeds authorized access'' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7)

the term ''department of the United States'' means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8)

the term ''damage'' means any impairment to the integrity or availability of data, a program, a system, or information;

(9)

the term ''government entity'' includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10)

the term ''conviction'' shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11)

the term ''loss'' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12)

corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f)

This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g)

Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h)

The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5)

TITLE 18 > PART I > CHAPTER 95 > Sec. 1956.

Prev | Next

Sec. 1956. - Laundering of monetary instruments

(a)

(1)

Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity -

(A)

(i)

with the intent to promote the carrying on of specified unlawful activity; or

(ii)

with intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or

(B)

knowing that the transaction is designed in whole or in part -

(i)

to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii)

to avoid a transaction reporting requirement under State or Federal law, shall be sentenced to a fine of not more than $500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both.

(2)

Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary

in the United States from or through a place outside the United States -

(A)

with the intent to promote the carrying on of specified unlawful activity; or

(B)

knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part -

(i)

to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii)

to avoid a transaction reporting requirement under State or Federal law, shall be sentenced to a fine of not more than $500,000 or twice the value of the monetary instrument or funds involved in the transportation, transmission, or transfer, whichever is greater, or imprisonment for not more than twenty years, or both. For the purpose of the offense described in subparagraph (B), the defendant's knowledge may be established by proof that a law enforcement officer represented the matter specified in subparagraph (B) as true, and the defendant's subsequent statements or actions indicate that the defendant believed such representations to be true.

(3)

Whoever, with the intent -

(A)

unlawful activity;

(B)

to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity; or

(C)

to avoid a transaction reporting requirement under State or

Federal law,

conducts or attempts to conduct a financial transaction involving property represented to be the proceeds of specified unlawful activity, or property used to conduct or facilitate specified unlawful activity, shall be fined under this title or imprisoned for not more than 20 years, or both. For purposes of this paragraph and paragraph (2), the term ''represented'' means any representation made by a law enforcement officer or by another person at the direction of, or with the approval of, a Federal official authorized to investigate or prosecute violations of this section.

(b) Penalties. -

(1) In general. -

Whoever conducts or attempts to conduct a transaction described in subsection (a)(1) or (a)(3), or section 1957, or a transportation, transmission, or transfer described in subsection (a)(2), is liable to the United States for a civil penalty of not more than the greater of -

(A)

the value of the property, funds, or monetary instruments involved in the transaction; or

(B)

$10,000.

(2) Jurisdiction over foreign persons. -

district courts shall have jurisdiction over any foreign person, including any financial institution authorized under the laws of a foreign country, against whom the action is brought, if service of process upon the foreign person is made under the Federal Rules of Civil Procedure or the laws of the country in which the foreign person is found, and -

(A)

the foreign person commits an offense under subsection (a) involving a financial transaction that occurs in whole or in part in the United States;

(B)

the foreign person converts, to his or her own use, property in which the United States has an ownership interest by virtue of the entry of an order of forfeiture by a court of the United States; or

(C)

the foreign person is a financial institution that maintains a bank account at a financial institution in the United States.

(3) Court authority over assets. -

A court described in paragraph (2) may issue a pretrial restraining order or take any other action necessary to ensure that any bank account or other property held by the defendant in the United States is available to satisfy a judgment under this section.

(4) Federal receiver. -

(A) In general. -

A court described in paragraph (2) may appoint a Federal Receiver, in accordance with subparagraph (B) of this paragraph, to collect, marshal, and take custody, control, and possession of all assets of the defendant, wherever located, to satisfy a civil judgment under this subsection, a forfeiture judgment under section 981 or 982, or a criminal sentence under section 1957 or subsection (a) of this section, including an order of restitution to any victim of a specified unlawful activity.

(B) Appointment and authority. -

A Federal Receiver described in subparagraph (A) -

(i)

may be appointed upon application of a Federal prosecutor or a Federal or State regulator, by the court having jurisdiction over the defendant in the case;

(ii)

shall be an officer of the court, and the powers of the Federal Receiver shall include the powers set out in section 754 of title 28, United States Code; and

(iii)

shall have standing equivalent to that of a Federal prosecutor for the purpose of submitting requests to obtain information regarding the assets of the defendant -

(I)

from the Financial Crimes Enforcement Network of the Department of the Treasury; or

(II)

from a foreign country pursuant to a mutual legal assistance treaty, multilateral agreement, or other arrangement for international law enforcement assistance, provided that such requests are in accordance with the policies and procedures of the Attorney General.

(c)

As used in this section -

(1)

financial transaction represents the proceeds of some form of unlawful activity'' means that the person knew the property involved in the transaction represented proceeds from some form, though not necessarily which form, of activity that constitutes a felony under State, Federal, or foreign law, regardless of whether or not such activity is specified in paragraph (7);

(2)

the term ''conducts'' includes initiating, concluding, or participating in initiating, or concluding a transaction;

(3)

the term ''transaction'' includes a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, use of a safe deposit box, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected;

(4)

the term ''financial transaction'' means

(A)

a transaction which in any way or degree affects interstate or foreign commerce

(i)

involving the movement of funds by wire or other means or

(ii)

involving one or more monetary instruments, or

(iii)

involving the transfer of title to any real property, vehicle, vessel, or aircraft, or

(B)

a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree;

(5)

the term ''monetary instruments'' means

(i)

coin or currency of the United States or of any other country, travelers' checks, personal checks, bank checks, and money orders, or

(ii)

investment securities or negotiable instruments, in bearer form or otherwise in such form that title thereto passes upon delivery;

(6)

the term ''financial institution'' includes -

(A)

any financial institution, as defined in section 5312(a)(2) of title 31, United States Code, or the regulations promulgated thereunder; and

(B)

any foreign bank, as defined in section 1 of the International Banking Act of 1978 (12 U.S.C. 3101).

(7)

the term ''specified unlawful activity'' means -

(A)

any act or activity constituting an offense

53 of title 31;

(B)

with respect to a financial transaction occurring in whole or in part in the United States, an offense against a foreign nation involving -

(i)

the manufacture, importation, sale, or distribution of a controlled substance (as such term is defined for the purposes of the Controlled Substances Act);

(ii)

murder, kidnapping, robbery, extortion, destruction of property by means of explosive or fire, or a crime of violence (as defined in section 16);

(iii)

fraud, or any scheme or attempt to defraud, by or against a foreign bank (as defined in paragraph 7 of section 1(b) of the International Banking Act of 1978)); [1]

(iv)

bribery of a public official, or the misappropriation, theft, or embezzlement of public funds by or for the benefit of a public official;

(v)

smuggling or export control violations involving -

(I)

an item controlled on the United States Munitions List established under section 38 of the Arms Export Control Act (22 U.S.C. 2778); or

(II)

an item controlled under regulations under the Export Administration Regulations (15 C.F.R. Parts 730-774); or

(vi)

an offense with respect to which the United States would be obligated by a multilateral treaty, either to extradite the alleged offender or to submit the case for prosecution, if the offender were found within the territory of the United States;

(C)

any act or acts constituting a continuing criminal enterprise, as that term is defined in section 408 of the Controlled Substances Act (21 U.S.C. 848);

(D)

an offense under section 32 (relating to the destruction of aircraft), section 37 (relating to violence at international airports), section 115 (relating to influencing, impeding, or retaliating against a Federal official by threatening or injuring a family member), section 152 (relating to concealment of assets; false oaths and claims; bribery), section 215 (relating to commissions or gifts for procuring loans), section 351 (relating to congressional or Cabinet officer assassination), any of sections 500 through 503 (relating to certain counterfeiting offenses), section 513 (relating to securities of States and private entities), section 541 (relating to goods falsely classified), section 542 (relating to entry of goods by means of false statements), section 545 (relating to smuggling goods into the United States), section 549 (relating to removing goods from Customs custody), section 641 (relating to public money, property, or records), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), section 657 (relating to lending, credit, and insurance institutions), section 658 (relating to property mortgaged or pledged to farm credit agencies), section 666 (relating to theft or bribery concerning programs receiving Federal funds),

involving nuclear materials), section 844(f) or (i) (relating to destruction by explosives or fire of Government property or property affecting interstate or foreign commerce), section 875 (relating to interstate communications), section 922(l) (relating to the unlawful importation of firearms), section 924(n) (relating to firearms trafficking), section 956 (relating to conspiracy to kill, kidnap, maim, or injure certain property in a foreign country), section 1005 (relating to fraudulent bank entries), 1006 [2] (relating to fraudulent Federal credit institution entries), 1007 (FOOTNOTE 2) (relating to Federal Deposit Insurance transactions), 1014 (FOOTNOTE 2) (relating to fraudulent loan or credit applications), section 1030 (relating to computer fraud and abuse), 1032 (FOOTNOTE 2) (relating to concealment of assets from conservator, receiver, or liquidating agent of financial institution), section 1111 (relating to murder), section 1114 (relating to murder of United States law enforcement officials), section 1116 (relating to murder of foreign officials, official guests, or internationally protected persons), section 1201 (relating to kidnaping), section 1203 (relating to hostage taking), section 1361 (relating to willful injury of Government property), section 1363 (relating to destruction of property within the special maritime and territorial jurisdiction), section 1708 (theft from the mail), section 1751 (relating to Presidential assassination), section 2113 or 2114 (relating to bank and postal robbery and theft), section 2280 (relating to violence against maritime navigation), section 2281 (relating to violence against maritime fixed platforms), section 2319 (relating to copyright infringement), section 2320 (relating to trafficking in counterfeit goods and services),, (FOOTNOTE 3) section 2332 (relating to terrorist acts abroad against United States nationals), section 2332a (relating to use of weapons of mass destruction), section 2332b (relating to international terrorist acts transcending national boundaries), or section 2339A or 2339B (relating to providing material support to terrorists) of this title, section 46502 of title 49, United States Code,, [3] a felony violation of the Chemical Diversion and Trafficking Act of 1988 (relating to precursor and essential chemicals), section 590 of the Tariff Act of 1930 (19 U.S.C. 1590) (relating to aviation smuggling), section 422 of the Controlled Substances Act (relating to transportation of drug

11 (relating to violations) of the Export Administration Act of 1979, section 206 (relating to penalties) of the International Emergency Economic Powers Act, section 16 (relating to offenses and punishment) of the Trading with the Enemy Act, any felony violation of section 15 of the Food Stamp Act of 1977 (relating to food stamp fraud) involving a quantity of coupons having a value of not less than $5,000, any violation of section 543(a)(1) of the Housing Act of 1949 (relating to equity skimming), any felony violation of the Foreign Agents Registration Act of 1938, or any felony violation of the Foreign Corrupt Practices Act; or ''section''.

ENVIRONMENTAL CRIMES

(E)

a felony violation of the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), the Ocean Dumping Act (33 U.S.C. 1401 et seq.), the Act to Prevent Pollution from Ships (33 U.S.C. 1901 et seq.), the Safe Drinking Water Act (42 U.S.C. 300f et seq.), or the Resources Conservation and Recovery Act (42 U.S.C. 6901 et seq.).

(F)

Any [4] act or activity constituting an offense involving a Federal health care offense.

(8)

the term ''State'' includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(d)

Nothing in this section shall supersede any provision of Federal, State, or other law imposing criminal penalties or affording civil remedies in addition to those provided for in this section.

(e)

Violations of this section may be investigated by such components of the Department of Justice as the Attorney

may direct, as appropriate and, with respect to offenses over which the United States Postal Service has jurisdiction, by the Postal Service. Such authority of the Secretary of the Treasury and the Postal Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury, the Postal Service, and the Attorney General. Violations of this section involving offenses described in paragraph (c)(7)(E) may be investigated by such components of the Department of Justice as the Attorney General may direct, and the National Enforcement Investigations Center of the Environmental Protection Agency.

(f)

There is extraterritorial jurisdiction over the conduct prohibited by this section if -

(1)

the conduct is by a United States citizen or, in the case of a non-United States citizen, the conduct occurs in part in the United States; and

(2)

the transaction or series of related transactions involves funds or monetary instruments of a value exceeding $10,000.

(g) Notice of Conviction of Financial Institutions. -

If any financial institution or any officer, director, or employee of any financial institution has been found guilty of an offense under this section, section 1957 or 1960 of this title, or section 5322 or 5324 of title 31, the Attorney General shall provide written notice of such fact to the appropriate regulatory agency for the financial institution.

(h)

Any person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

(i) Venue. -

(1)

brought in -

(A)

any district in which the financial or monetary transaction is conducted; or

(B)

any district where a prosecution for the underlying specified unlawful activity could be brought, if the defendant participated in the transfer of the proceeds of the specified unlawful activity from that district to the district where the financial or monetary transaction is conducted.

(2)

A prosecution for an attempt or conspiracy offense under this section or section 1957 may be brought in the district where venue would lie for the completed offense under paragraph (1), or in any other district where an act in furtherance of the attempt or conspiracy took place.

(3)

For purposes of this section, a transfer of funds from 1 place to another, by wire or any other means, shall constitute a single, continuing transaction. Any person who conducts (as that term is defined in subsection (c)(2)) any portion of the transaction may be charged in any district in which the transaction takes place

---

TITLE 18 > PART I > CHAPTER 95 > Sec. 1957.

Prev | Next

Sec. 1957. - Engaging in monetary transactions in property derived from specified unlawful activity

(a)

Whoever, in any of the circumstances set forth in subsection (d), knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity, shall be punished as provided in subsection (b).

(b)

(1)

Except as provided in paragraph (2), the punishment for an offense under this section is a fine under title 18, United States Code, or imprisonment for not more than ten years or both.

(2)

The court may impose an alternate fine to that imposable under paragraph (1) of not more than twice the amount of the criminally derived property involved in the transaction.

(c)

In a prosecution for an offense under this section, the Government is not required to prove the defendant knew that the offense from which the criminally derived property was derived was specified unlawful activity.

(d)

The circumstances referred to in subsection (a) are -

(1)

jurisdiction of the United States; or

(2)

that the offense under this section takes place outside the United States and such special jurisdiction, but the defendant is a United States person (as defined in section 3077 of this title, but excluding the class described in paragraph (2)(D) of such section).

(e)

Violations of this section may be investigated by such components of the Department of Justice as the Attorney General may direct, and by such components of the Department of the Treasury as the Secretary of the Treasury may direct, as appropriate and, with respect to offenses over which the United States Postal Service has jurisdiction, by the Postal Service. Such authority of the Secretary of the Treasury and the Postal Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury, the Postal Service, and the Attorney General.

(f)

As used in this section -

(1)

the term ''monetary transaction'' means the deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument (as defined in section 1956(c)(5) of this title) by, through, or to a financial institution (as defined in section 1956 of this title), including any transaction that would be a financial transaction under section 1956(c)(4)(B) of this title, but such term does not include any transaction necessary to preserve a person's right to representation as guaranteed by the sixth amendment to the Constitution;

(2)

the term ''criminally derived property'' means any property constituting, or derived from, proceeds obtained from a criminal offense; and

(3)

the term ''specified unlawful activity'' has the meaning given that term in section 1956 of this title

Sec. 1960. - Prohibition of unlicensed money transmitting businesses

(a)

Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.

(b)

As used in this section -

(1)

the term ''unlicensed money transmitting business'' means a money transmitting business which affects interstate or foreign commerce in any manner or degree and -

(A)

is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable;

(B)

fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or

(C)

otherwise involves the transportation or transmission of funds that are known to the

promote or support unlawful activity;

(2)

the term ''money transmitting'' includes transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier; and

(3)

the term ''State'' means any State of the United States, the District of Columbia, the Northern Mariana Islands, and any commonwealth, territory, or possession of the United States

---

TITLE 18 > PART I > CHAPTER 46 > Sec. 981. Next

Sec. 981. - Civil forfeiture

(a)

(1)

The following property is subject to forfeiture to the United States:

(A)

Any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title, or any property traceable to such property.

(B)

Any property, real or personal, within the

obtained directly or indirectly from an offense against a foreign nation, or any property used to facilitate such an offense, if the offense -

(i)

involves the manufacture, importation, sale, or distribution of a controlled substance (as that term is defined for purposes of the Controlled Substances Act), or any other conduct described in section 1956(c)(7)(B);

(ii)

would be punishable within the jurisdiction of the foreign nation by death or imprisonment for a term exceeding 1 year; and

(iii)

would be punishable under the laws of the United States by imprisonment for a term exceeding 1 year, if the act or activity constituting the offense had occurred within the jurisdiction of the United States.

(C)

Any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of section 215, 471, 472, 473, 474, 476, 477, 478, 479, 480, 481, 485, 486, 487, 488, 501, 502, 510, 542, 545, 656, 657, 842, 844, 1005, 1006, 1007, 1014, 1028, 1029, 1030, 1032, or 1344 of this title or any offense constituting ''specified unlawful activity'' (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense.

(D)

Any property, real or personal, which represents or is traceable to the gross receipts obtained, directly or indirectly, from a violation of -

(i)

section 666(a)(1) (relating to Federal program fraud);

(ii)

section 1001 (relating to fraud and false statements);

(iii)

section 1031 (relating to major fraud against the United States);

(iv)

section 1032 (relating to concealment of assets from conservator or receiver of insured financial institution);

(v)

section 1341 (relating to mail fraud); or

(vi)

section 1343 (relating to wire fraud),

if such violation relates to the sale of assets acquired or held by the Resolution Trust Corporation, the Federal Deposit Insurance Corporation, as conservator or receiver for a financial institution, or any other conservator for a financial institution appointed by the Office of the Comptroller of the Currency or the Office of Thrift Supervision or the National Credit Union Administration, as conservator or liquidating agent for a financial institution.

(E)

With respect to an offense listed in subsection (a)(1)(D) committed for the purpose of executing or attempting to execute any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent statements, pretenses, representations or promises, the gross receipts of such an offense shall include all property, real or personal, tangible or intangible, which thereby is obtained, directly or indirectly.

(F)

obtained, directly or indirectly, from a violation of -

(i)

section 511 (altering or removing motor vehicle identification numbers);

(ii)

section 553 (importing or exporting stolen motor vehicles);

(iii)

section 2119 (armed robbery of automobiles);

(iv)

section 2312 (transporting stolen motor vehicles in interstate commerce); or

(v)

section 2313 (possessing or selling a stolen motor vehicle that has moved in interstate commerce).

(G)

All assets, foreign or domestic -

(i)

of any individual, entity, or organization engaged in planning or perpetrating any act of domestic or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property, and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization;

(ii)

acquired or maintained by any person with the intent and for the purpose of supporting, planning, conducting, or concealing an act of

States, citizens or residents of the United States, or their property; or

(iii)

derived from, involved in, or used or intended to be used to commit any act of domestic or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property.

(2)

For purposes of paragraph (1), the term ''proceeds'' is defined as follows:

(A)

In cases involving illegal goods, illegal services, unlawful activities, and telemarketing and health care fraud schemes, the term ''proceeds'' means property of any kind obtained directly or indirectly, as the result of the commission of the offense giving rise to forfeiture, and any property traceable thereto, and is not limited to the net gain or profit realized from the offense.

(B)

In cases involving lawful goods or lawful services that are sold or provided in an illegal manner, the term ''proceeds'' means the amount of money acquired through the illegal transactions resulting in the forfeiture, less the direct costs incurred in providing the goods or services. The claimant shall have the burden of proof with respect to the issue of direct costs. The direct costs shall not include any part of the overhead expenses of the entity providing the goods or services, or any part of the income taxes paid by the entity.

(C)

In cases involving fraud in the process of obtaining a loan or extension of credit, the court shall allow the claimant a deduction from the forfeiture to the extent that the loan was repaid, or the debt was satisfied, without any financial loss to the victim.

(b)

(1)

Except as provided in section 985, any property subject to forfeiture to the United States under subsection (a) may be seized by the Attorney General and, in the case of property involved in a violation investigated by the Secretary of the Treasury or the United States Postal Service, the property may also be seized by the Secretary of the Treasury or the Postal Service, respectively.

(2)

Seizures pursuant to this section shall be made pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure, except that a seizure may be made without a warrant if -

(A)

a complaint for forfeiture has been filed in the United States district court and the court issued an arrest warrant in rem pursuant to the Supplemental Rules for Certain Admiralty and Maritime Claims;

(B)

there is probable cause to believe that the property is subject to forfeiture and -

(i)

the seizure is made pursuant to a lawful arrest or search; or

(ii)

another exception to the Fourth Amendment warrant requirement would apply; or

(C)

the property was lawfully seized by a State or local law enforcement agency and transferred to a Federal agency.

(3)

Notwithstanding the provisions of rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1355(b) of title 28, and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement. Any motion for the return of property seized under this section shall be filed in the district court in which the seizure warrant was issued or in the district court for the district in which the property was seized.

(4)

(A)

If any person is arrested or charged in a foreign country in connection with an offense that would give rise to the forfeiture of property in the United States under this section or under the Controlled Substances Act, the Attorney General may apply to any Federal judge or magistrate judge in the district in which the property is located for an ex parte order restraining the property subject to forfeiture for not more than 30 days, except that the time may be extended for good cause shown at a hearing conducted in the manner provided in rule 43(e) of the Federal Rules of Civil Procedure.

(B)

The application for the restraining order shall set forth the nature and circumstances of the foreign charges and the basis for belief that the person arrested or charged has property in the United States that would be subject to forfeiture, and shall contain a statement that the restraining order is needed to preserve the availability of property for such time as is necessary to receive evidence from the foreign country or elsewhere in support of probable cause for the seizure of the property under this subsection.

(c)

Property taken or detained under this section shall not be

Service, as the case may be, subject only to the orders and decrees of the court or the official having jurisdiction thereof. Whenever property is seized under this subsection, the Attorney General, the Secretary of the Treasury, or the Postal Service, as the case may be, may -

(1)

place the property under seal;

(2)

remove the property to a place designated by him; or

(3)

require that the General Services Administration take custody of the property and remove it, if practicable, to an appropriate location for disposition in accordance with law.

(d)

For purposes of this section, the provisions of the customs laws relating to the seizure, summary and judicial forfeiture, condemnation of property for violation of the customs laws, the disposition of such property or the proceeds from the sale of this section, the remission or mitigation of such forfeitures, and the compromise of claims (19 U.S.C. 1602 et seq.), insofar as they are applicable and not inconsistent with the provisions of this section, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under this section, except that such duties as are imposed upon the customs officer or any other person with respect to the seizure and forfeiture of property under the customs laws shall be performed with respect to seizures and forfeitures of property under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General, the Secretary of the Treasury, or the Postal Service, as the case may be. The Attorney General shall have sole responsibility for disposing of petitions for remission or mitigation with respect to property involved in a judicial forfeiture proceeding.

(e)

Notwithstanding any other provision of the law, except section 3 of the Anti Drug Abuse Act of 1986, the Attorney General, the Secretary of the Treasury, or the Postal Service, as

terms and conditions as he may determine -

(1)

to any other Federal agency;

(2)

to any State or local law enforcement agency which participated directly in any of the acts which led to the seizure or forfeiture of the property;

(3)

in the case of property referred to in subsection (a)(1)(C), to any Federal financial institution regulatory agency -

(A)

to reimburse the agency for payments to claimants or creditors of the institution; and

(B)

to reimburse the insurance fund of the agency for losses suffered by the fund as a result of the receivership or liquidation;

(4)

in the case of property referred to in subsection (a)(1)(C), upon the order of the appropriate Federal financial institution regulatory agency, to the financial institution as restitution, with the value of the property so transferred to be set off against any amount later recovered by the financial institution as compensatory damages in any State or Federal proceeding;

(5)

in the case of property referred to in subsection (a)(1)(C), to any Federal financial institution regulatory agency, to the extent of the agency's contribution of resources to, or expenses involved in, the seizure and forfeiture, and the investigation leading directly to the seizure and forfeiture, of such property;

(6)

as restoration to any victim of the offense giving rise to the forfeiture, including, in the case of a money laundering offense, any offense constituting the underlying specified unlawful activity; or

(7)

In [1] the case of property referred to in subsection (a)(1)(D), to the Resolution Trust Corporation, the Federal Deposit Insurance Corporation, or any other Federal financial institution regulatory agency (as defined in section 8(e)(7)(D) of the Federal Deposit Insurance Act). The Attorney General, the Secretary of the Treasury, or the Postal Service, as the case may be, shall ensure the equitable transfer pursuant to paragraph (2) of any forfeited property to the appropriate State or local law enforcement agency so as to reflect generally the contribution of any such agency participating directly in any of the acts which led to the seizure or forfeiture of such property. A decision by the Attorney General, the Secretary of the Treasury, or the Postal Service pursuant to paragraph (2) shall not be subject to review. The United States shall not be liable in any action arising out of the use of any property the custody of which was transferred pursuant to this section to any non-Federal agency. The Attorney General, the Secretary of the Treasury, or the Postal Service may order the discontinuance of any forfeiture proceedings under this section in favor of the institution of forfeiture proceedings by State or local authorities under an appropriate State or local statute. After the filing of a complaint for forfeiture under this section, the Attorney General may seek dismissal of the complaint in favor of forfeiture proceedings under State or local law. Whenever forfeiture proceedings are discontinued by the United States in favor of State or local proceedings, the United States may transfer custody and possession of the seized property to the appropriate State or local official immediately upon the initiation of the proper actions by such officials. Whenever forfeiture proceedings are discontinued by the United States in favor of State or local proceedings, notice shall be sent to all known interested parties advising them of the discontinuance or dismissal. The United States shall not be liable in any action arising out of the seizure, detention, and transfer of seized property to State or local officials. The United States shall not be liable in any action arising out of a transfer under paragraph (3), (4), or (5) of this subsection.

(f)

All right, title, and interest in property described in subsection (a) of this section shall vest in the United States upon commission of the act giving rise to forfeiture under this section.

(g)

(1)

Upon the motion of the United States, the court shall stay the civil forfeiture proceeding if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related criminal investigation or the prosecution of a related criminal case.

(2)

Upon the motion of a claimant, the court shall stay the civil forfeiture proceeding with respect to that claimant if the court determines that -

(A)

the claimant is the subject of a related criminal investigation or case;

(B)

the claimant has standing to assert a claim in the civil forfeiture proceeding; and

(C)

continuation of the forfeiture proceeding will burden the right of the claimant against self-incrimination in the related investigation or case.

(3)

With respect to the impact of civil discovery described in paragraphs (1) and (2), the court may determine that a stay is unnecessary if a protective order limiting discovery would protect the interest of one party without unfairly limiting the ability of the opposing party to pursue the civil case. In no case, however, shall the court impose a protective order as an alternative to a stay

substantially unable to do so.

(4)

In this subsection, the terms ''related criminal case'' and ''related criminal investigation'' mean an actual prosecution or investigation in progress at the time at which the request for the stay, or any subsequent motion to lift the stay is made. In determining whether a criminal case or investigation is ''related'' to a civil forfeiture proceeding, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the two proceedings, without requiring an identity with respect to any one or more factors.

(5)

In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect an ongoing criminal investigation or pending criminal trial.

(6)

Whenever a civil forfeiture proceeding is stayed pursuant to this subsection, the court shall enter any order necessary to preserve the value of the property or to protect the rights of lienholders or other persons with an interest in the property while the stay is in effect.

(7)

A determination by the court that the claimant has standing to request a stay pursuant to paragraph (2) shall apply only to this subsection and shall not preclude the Government from objecting to the standing of the claimant by dispositive motion or at the time of trial.

(h)

In addition to the venue provided for in section 1395 of title 28 or any other provision of law, in the case of property of a defendant charged with a violation that is the basis for forfeiture of the property under this section, a proceeding for forfeiture under this section may be brought in the judicial district in which the defendant owning such property is found or in the judicial district in which the criminal prosecution is brought.

(i)

(1)

Whenever property is civilly or criminally forfeited under this chapter, the Attorney General or the Secretary of the Treasury, as the case may be, may transfer the forfeited personal property or the proceeds of the sale of any forfeited personal or real property to any foreign country which participated directly or indirectly in the seizure or forfeiture of the property, if such a transfer -

(A)

has been agreed to by the Secretary of State;

(B)

is authorized in an international agreement between the United States and the foreign country; and

(C)

is made to a country which, if applicable, has been certified under section 481(h) [2] of the Foreign Assistance Act of 1961.

A decision by the Attorney General or the Secretary of the Treasury pursuant to this paragraph shall not be subject to review. The foreign country shall, in the event of a transfer of property or proceeds of sale of property under this subsection, bear all expenses incurred by the United States in the seizure, maintenance, inventory, storage, forfeiture, and disposition of the property, and all transfer costs. The payment of all such expenses, and the transfer of assets pursuant to this paragraph, shall be upon such terms and conditions as the Attorney General or the Secretary of the Treasury may, in his discretion, set.

(2)

The provisions of this section shall not be construed as limiting or superseding any other authority of the United States to provide assistance to a foreign country in obtaining property related to a crime committed in the foreign country, including property which is sought as evidence of a crime committed in the foreign country.

(3)

property which is the subject of forfeiture under this section and was determined by such court to be the type of property described in subsection (a)(1)(B) of this section, and any certified recordings or transcripts of testimony taken in a foreign judicial proceeding concerning such order or judgment of forfeiture, shall be admissible in evidence in a proceeding brought pursuant to this section. Such certified order or judgment of forfeiture, when admitted into evidence, shall constitute probable cause that the property forfeited by such order or judgment of forfeiture is subject to forfeiture under this section and creates a rebuttable presumption of the forfeitability of such property under this section.

(4)

A certified order or judgment of conviction by a court of competent jurisdiction of a foreign country concerning an unlawful drug activity which gives rise to forfeiture under this section and any certified recordings or transcripts of testimony taken in a foreign judicial proceeding concerning such order or judgment of conviction shall be admissible in evidence in a proceeding brought pursuant to this section. Such certified order or judgment of conviction, when admitted into evidence, creates a rebuttable presumption that the unlawful drug activity giving rise to forfeiture under this section has occurred.

(5)

The provisions of paragraphs (3) and (4) of this subsection shall not be construed as limiting the admissibility of any evidence otherwise admissible, nor shall they limit the ability of the United States to establish probable cause that property is subject to forfeiture by any evidence otherwise admissible.

(j)

For purposes of this section -

(1)

the term ''Attorney General'' means the Attorney General or his delegate; and

(2)

Secretary of the Treasury or his delegate.

(k) Interbank Accounts. -

(1) In general. -

(A) In general. -

For the purpose of a forfeiture under this section or under the Controlled Substances Act (21 U.S.C. 801 et seq.), if funds are deposited into an account at a foreign bank, and that foreign bank has an interbank account in the United States with a covered financial institution (as defined in section 5318(j)(1) of title 31), the funds shall be deemed to have been deposited into the interbank account in the United States, and any restraining order, seizure warrant, or arrest warrant in rem regarding the funds may be served on the covered financial institution, and funds in the interbank account, up to the value of the funds deposited into the account at the foreign bank, may be restrained, seized, or arrested.

(B) Authority to suspend. -

The Attorney General, in consultation with the Secretary of the Treasury, may suspend or terminate a forfeiture under this section if the Attorney General determines that a conflict of law exists between the laws of the jurisdiction in which the foreign bank is located and the laws of the United States with respect to liabilities arising from the restraint, seizure, or arrest of such funds, and that such suspension or termination would be in the interest of justice and would not harm the national interests of the United States.

(2) No requirement for government to trace funds. -

If a forfeiture action is brought against funds that are restrained, seized, or arrested under paragraph (1), it shall not be necessary for the Government to establish that the funds are directly traceable to the funds that were deposited into the foreign bank, nor shall it be necessary for the Government to rely on the application of section 984.

(3) Claims brought by owner of the funds. -

restrained, seized, or arrested under paragraph (1), the owner of the funds deposited into the account at the foreign bank may contest the forfeiture by filing a claim under section 983.

(4) Definitions. -

For purposes of this subsection, the following definitions shall apply:

(A) Interbank account. -

The term ''interbank account'' has the same meaning as in section 984(c)(2)(B).

(B) Owner. -

(i) In general. -

Except as provided in clause (ii), the term ''owner'' -

(I)

means the person who was the owner, as that term is defined in section 983(d)(6), of the funds that were deposited into the foreign bank at the time such funds were deposited; and

(II)

does not include either the foreign bank or any financial institution acting as an intermediary in the transfer of the funds into the interbank account.

(ii) Exception. -

The foreign bank may be considered the ''owner'' of the funds (and no other person shall qualify as the owner of such funds) only if -

(I)

the basis for the forfeiture action is wrongdoing committed by the foreign bank; or

(II)

the foreign bank establishes, by a preponderance of the evidence, that prior to the restraint, seizure, or arrest of the funds, the foreign bank had discharged all or part of its obligation to the prior owner of the funds, in which case the foreign bank shall be deemed the owner of the funds to the extent of such discharged obligation

TITLE 18 > PART I > CHAPTER 46 > Sec. 982.

Prev | Next

Sec. 982. - Criminal forfeiture

(a)

(1)

The court, in imposing sentence on a person convicted of an offense in violation of section 1956, 1957, or 1960 of this title, shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property.

(2)

The court, in imposing sentence on a person convicted of a violation of, or a conspiracy to violate -

(A)

section 215, 656, 657, 1005, 1006, 1007, 1014, 1341, 1343, or 1344 of this title, affecting a financial institution, or

(B)

section 471, 472, 473, 474, 476, 477, 478, 479, 480, 481, 485, 486, 487, 488, 501, 502, 510, 542, 545, 842, 844, 1028, 1029, or 1030 of this title,

shall order that the person forfeit to the United States any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of such violation.

(3)

The court, in imposing a sentence on a person convicted of an offense under -

(A)

section 666(a)(1) (relating to Federal program fraud);

(B)

section 1001 (relating to fraud and false statements);

(C)

section 1031 (relating to major fraud against the United States);

(D)

section 1032 (relating to concealment of assets from conservator, receiver, or liquidating agent of insured financial institution);

(E)

section 1341 (relating to mail fraud); or

(F)

section 1343 (relating to wire fraud),

involving the sale of assets acquired or held by the Resolution Trust Corporation, the Federal Deposit Insurance Corporation, as conservator or receiver for a financial institution or any other conservator for a financial institution

Administration, as conservator or liquidating agent for a financial institution, shall order that the person forfeit to the United States any property, real or personal, which represents or is traceable to the gross receipts obtained, directly or indirectly, as a result of such violation.

(4)

With respect to an offense listed in subsection (a)(3) committed for the purpose of executing or attempting to execute any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent statements, pretenses, representations, or promises, the gross receipts of such an offense shall include any property, real or personal, tangible or intangible, which is obtained, directly or indirectly, as a result of such offense.

(5)

The court, in imposing sentence on a person convicted of a violation or conspiracy to violate -

(A)

section 511 (altering or removing motor vehicle identification numbers);

(B)

section 553 (importing or exporting stolen motor vehicles);

(C)

section 2119 (armed robbery of automobiles);

(D)

section 2312 (transporting stolen motor vehicles in interstate commerce); or

(E)

section 2313 (possessing or selling a stolen motor vehicle that has moved in interstate commerce);

the gross proceeds obtained, directly or indirectly, as a result of such violation.

(6)

(A)

The court, in imposing sentence on a person convicted of a violation of, or conspiracy to violate, section 274(a), 274A(a)(1), or 274A(a)(2) of the Immigration and Nationality Act or section 1425, 1426, 1427, 1541, 1542, 1543, 1544, or 1546 of this title, or a violation of, or conspiracy to violate, section 1028 of this title if committed in connection with passport or visa issuance or use, shall order that the person forfeit to the United States, regardless of any provision of State law -

(i)

any conveyance, including any vessel, vehicle, or aircraft used in the commission of the offense of which the person is convicted; and

(ii)

any property real or personal -

(I)

that constitutes, or is derived from or is traceable to the proceeds obtained directly or indirectly from the commission of the offense of which the person is convicted; or

(II)

that is used to facilitate, or is intended to be used to facilitate, the commission of the offense of which the person is convicted.

(B)

The court, in imposing sentence on a person described in subparagraph (A), shall order that the person forfeit to the United States all property described in that subparagraph.

(7)

The court, in imposing sentence on a person convicted of a Federal health care offense, shall order the person to forfeit property, real or personal, that constitutes or is derived, directly or indirectly, from gross proceeds traceable to the commission of the offense.

(8)

The Court, [1] in sentencing a defendant convicted of an offense under section 1028, 1029, 1341, 1342, 1343, or 1344, or of a conspiracy to commit such an offense, if the offense involves telemarketing (as that term is defined in section 2325), shall order that the defendant forfeit to the United States any real or personal property -

(A)

used or intended to be used to commit, to facilitate, or to promote the commission of such offense; and

(B)

constituting, derived from, or traceable to the gross proceeds that the defendant obtained directly or indirectly as a result of the offense.

(b)

(1)

The forfeiture of property under this section, including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 (other than subsection (d) of that section) of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853).

(2)

The substitution of assets provisions of subsection 413(p) shall not be used to order a defendant to forfeit assets in place of the actual property laundered where such defendant acted merely as an intermediary who handled but did not retain the property in the course of

forfeiture, conducted three or more separate transactions involving a total of $100,000 or more in any twelve month period

Français

Convention on Cybercrime

Budapest, 23.XI.2001

Explanatory Report

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned at the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights, as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political

Rights, as well as other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the protection of personal data, as conferred e.g. by the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field as well as similar treaties which exist between Council of Europe member States and other States and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrimes, including actions of the United Nations, the OECD, the European Union and the G8;

Recalling Recommendation N° R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, Recommendation N° R (88) 2 on piracy in the field of copyright and neighbouring rights, Recommendation N° R (87) 15 regulating the use of personal data in the police sector, Recommendation N° R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services as well as Recommendation N° R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and Recommendation N° R (95) 13 concerning problems of criminal procedural law connected with Information Technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, June 1997), which recommended the Committee of Ministers to support the work carried out by the European Committee on Crime Problems (CDPC) on cybercrime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offences, as well as to Resolution N° 3, adopted at the 23rd Conference of the European Ministers of Justice (London, June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe, on the occasion of their Second Summit (Strasbourg, 10 - 11 October 1997), to seek common responses to the development of the new information technologies, based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a. "computer system" means any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c. "service provider" means:

i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

with intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5; and

b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2).

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:

a. any input, alteration, deletion or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a. producing child pornography for the purpose of its distribution through a computer system;

b. offering or making available child pornography through a computer system;

c. distributing or transmitting child pornography through a computer system;

d. procuring child pornography through a computer system for oneself or for another;

e. possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above "child pornography" shall include pornographic material that visually depicts:

a. a minor engaged in sexually explicit conduct;

b. a person appearing to be a minor engaged in sexually explicit conduct;

c. realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraph 1(d) and 1(e), and 2(b) and 2(c).

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations done in Rome (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 – 10 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9 (1) a and 9 (1) c of this Convention.

3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that a legal person can be held liable for a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

a. a power of representation of the legal person;

b. an authority to take decisions on behalf of the legal person;

c. an authority to exercise control within the legal person.

2. Apart from the cases already provided for in paragraph 1, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 – 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 to:

a. the criminal offences established in accordance with articles 2-11 of this Convention;

b. other criminal offences committed by means of a computer system; and

c. the collection of evidence in electronic form of a criminal offence.

3. a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system

i. is being operated for the benefit of a closed group of users, and

ii. does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, a Party shall consider the impact of the powers and procedures in this Section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 - Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative or other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control;

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, "subscriber information" means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers of its services, other than traffic or content data, by which can be established:

a. the type of the communication service used, the technical provisions taken thereto and the period of service;

b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c. any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a. a computer system or part of it and computer data stored therein; and

b. computer-data storage medium in which computer data may be stored

in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1 (a), and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to :

a. seize or similarly secure a computer system or part of it or a computer-data storage medium;

b. make and retain a copy of those computer data;

c. maintain the integrity of the relevant stored computer data; and

d. render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a. collect or record through application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications in its territory through application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a. collect or record through application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data of specified communications in its territory through application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 – 11 of this Convention, when the offence is committed :

a. in its territory; or

b. on board a ship flying the flag of that Party; or

c. on board an aircraft registered under the laws of that Party; or

d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs (1) b – (1) d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph (1) of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him/her to another Party, solely on the basis of his/her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1. a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 – 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this Article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as in the case of any other offence of a comparable nature under the law of that Party.

7. a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and addresses of each authority responsible for the making to or receipt of a request for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 - 35.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in Articles in this Chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 to 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1. A Party may, within the limits of its domestic law, without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2. Prior to providing such information, the providing Party may request that it be kept confidential or used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation is available, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. a. Each Party shall designate a central authority or authorities that shall be responsible for sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other.

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph.

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this Article shall be executed in accordance with the procedures specified by the requesting Party except where incompatible with the law of the requested Party.

4. The requested Party may, in addition to grounds for refusal available under Article 25, paragraph (4), refuse assistance if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. If the request is refused or postponed, reasons shall be given for the refusal or postponement. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact and substance of any request made under this Chapter except to the extent necessary to execute the request. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9. a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to subparagraph (a) and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation, is available unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the furnishing of information or material in response to a request dependent on the condition that it is:

a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b. not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information is nevertheless provided. When the requesting Party accepts the condition, it shall be bound by it.

4. Any Party that furnishes information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:

a. the authority that is seeking the preservation;

b. the offence that is the subject of a criminal investigation or proceeding and a brief summary of related facts;

c. the stored computer data to be preserved and its relationship to the offence;

d. any available information to identify the custodian of the stored computer data or the location of the computer system;

e. the necessity of the preservation; and

f. that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data may, in respect of offences other than those established in

accordance with Articles 2 – 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reason to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if :

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of, or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than 60 days in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made under Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if :

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2. The requested Party shall respond to the request through application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this Chapter.

3. The request shall be responded to on an expedited basis where:

a. there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b. the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without obtaining the authorisation of another Party:

a. access publicly available (open source) stored computer data**,** regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other with respect to the real-time collection of traffic data associated with specified communications in its territory transmitted by means of a computer system. Subject to paragraph 2, assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other with respect to the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted by their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1. Each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out:

a. provision of technical advice;

b. preservation of data pursuant to Articles 29 and 30; and

c. collection of evidence, giving of legal information, and locating of suspects.

2. a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20 (d) of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition opened for signature in Paris on 13 December 1957 (ETS No. 24);

- the European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 20 April 1959 (ETS No. 30);

- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or otherwise have established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Article 2, Article 3, Article 6, paragraph 1 (b), Article 7, Article 9, paragraph 3 and Article 27, paragraph 9 (e).

Article 41 – Federal clause

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the European Committee on Crime Problems (CDPC) and,

following consultation with the non-member State Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the European Committee on Crime Problems (CDPC), to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

a. the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b. the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c. consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The European Committee on Crime Problems (CDPC) shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this Article.

Article 47 – Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this Convention in accordance with Articles 36 and 37;

d. any declaration made under Article 40 or reservation made in accordance with Article 42;

e. any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวสุธาสินี พรหมมินทร์ เกิดวันที่ 23 พฤศจิกายน 2518 สำเร็จการศึกษาชั้นมัธยมศึกษาตอนปลาย จากโรงเรียนสตรีสมุทรปราการ และสำเร็จการศึกษาชั้นปริญญาตรี คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อปีการศึกษา 2539 ปัจจุบันปฏิบัติงานในตำแหน่ง เจ้าหน้าที่ประสานงานด้านกฎหมาย สำนักบัญชีและการเงินกลางด้านกฎหมาย บริษัท ซี.พี. เซเว่น อีเลฟเว่น จำกัด (มหาชน)