บทที่ 2

ความหมายและลักษณะการกระทำผิดที่เกี่ยวกับเครื่องหมายที่ใช้ระบุตัวบุคคล

เนื่องจากในปัจจุบันได้มีการนำเครื่องหมายที่ใช้ระบุตัวบุคคลประเภทต่างๆมาใช้อย่างแพร่หลาย ในบทนี้จะได้กล่าวถึงความหมายและลักษณะของการกระทำความผิดที่เกี่ยวกับเครื่องหมายที่ใช้ระบุตัวบุคคล โดยในส่วนแรกจะกล่าวถึงหลักการและเหตุผลความจำเป็นที่ต้องมีเครื่องหมายที่ใช้ระบุตัวบุคคล ในส่วนที่สองจะกล่าวถึงลักษณะของเครื่องหมายที่ใช้ระบุตัวบุคคลในประเภทต่างๆ เช่น รหัสข้อมูล บัตรอิเล็กทรอนิกส์ และลักษณะทางชีวภาพของบุคคล (Biometrics) และส่วนสุดท้ายจะได้อธิบายถึงสภาพปัญหาและรูปแบบของการกระทำความผิดที่เกี่ยวกับเครื่องหมายที่ใช้ระบุตัวบุคคลในประเภทต่างๆ ของกลุ่มคนร้ายเพื่อให้ได้มาและนำออกใช้ ซึ่งเครื่องหมายที่ใช้ระบุตัวบุคคลตั้งแต่ขั้นตอนการสมัครเพื่อขอใช้บริการ ขั้นตอนการจัดส่งหรือส่งมอบ และขั้นตอนของการใช้ อันเป็นการก่อให้เกิดความเสียหายที่กำลังทวีความรุนแรงยิ่งขึ้นในปัจจุบัน

2.1 หลักการและเหตุผล

เนื่องจากการติดต่อสื่อสารหรือทำธุรกรรมต่างๆระหว่างบุคคลจะต้องอาศัยความไว้เนื้อเชื่อใจระหว่างบุคคลเพื่อก่อให้เกิดนิติสัมพันธ์ ซึ่งมักจะเกิดขึ้นจากการที่คู่สัญญาจะต้องได้พบปะเห็นหน้ากันมาก่อน หรือคู่กรณีได้มาแสดงเจตนาต่อหน้าหรือโดยวิธีที่ถือเสมือนว่าอยู่ต่อหน้ากัน เช่น การโทรศัพท์พูดคุยกัน เป็นต้น ทำให้การทำธุรกรรมที่คู่สัญญาอยู่ห่างไกลกันทำได้ลำบากมาก เพราะต้องเดินทางเพื่อติดต่อกัน แต่ต่อมาเมื่อมีการนำระบบคอมพิวเตอร์และระบบเครือข่ายอินเตอร์เน็ตมาใช้อย่างแพร่หลายจึงทำให้เกิดรูปแบบการพาณิชย์แบบใหม่ขึ้นซึ่งรู้จักกันทั่วไปว่า "พาณิชย์อิเล็กทรอนิกส์" โดยมีการทำสัญญากันบนเครือข่าย (ONLINE CONTRACT) และปฏิวัติโฉมหน้าการซื้อขายสู่ยุค MOUSE AND CLICK บนหน้าจอคอมพิวเตอร์[1] เพราะสามารถทำได้ง่ายและประหยัดเวลาและค่าใช้จ่ายในการเดินทาง จึงทำให้ความสำคัญของการทำธุรกรรมที่คู่สัญญา

---

[1]วีระพงษ์ บุญโญภาส, อาชญากรรมทางเศรษฐกิจ, พิมพ์ครั้งที่ 4 (กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2547), น. 436.

จะต้องแสดงเจตนาสื่อสารกันโดยตรงลดน้อยลง แต่อย่างไรก็ดี เพื่อรักษาความปลอดภัยในการติดต่อสื่อสารระหว่างบุคคลและเพื่อให้แน่ใจว่าเป็นบุคคลที่ประสงค์จะติดต่อด้วยจึงต้องใช้สัญลักษณ์อื่นแทนเพราะไม่อาจพบหน้าและลงลายมือชื่อในสัญญาแบบเดิมได้ ซึ่งเรียกสัญลักษณ์ดังกล่าวว่า "เครื่องหมายที่ใช้ระบุตัวบุคคล (Authentication)" โดยมีวัตถุประสงค์เพื่อ[2]

1. การระบุตัว (Authentication) เพื่อยืนยันตัวบุคคลผู้ส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์

2. การควบคุมการเข้าถึง (Access Control) ซึ่งอนุญาตให้เฉพาะบุคคลที่มีสิทธิหรือได้รับอนุญาตเท่านั้นในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ และป้องกันมิให้บุคคลซึ่งไม่มีสิทธิหรือไม่ได้รับอนุญาตเข้าถึงข้อมูลนั้น

3. การรักษาความลับ (Confidentiality) เพื่อป้องกันมิให้บุคคลซึ่งไม่ได้รับอนุญาตหรือไม่มีสิทธิได้อ่านข้อมูลอิเล็กทรอนิกส์

4. ความถูกต้องครบถ้วนของข้อมูลอิเล็กทรอนิกส์ (Integrity) เพื่อป้องกันมิให้มีการเปลี่ยนแปลง แก้ไข ทำลาย หรือสร้างข้อมูลอิเล็กทรอนิกส์นั้นโดยไม่ได้รับอนุญาต

5. การป้องกันการปฏิเสธความรับผิด (Non - repudiation) เพื่อป้องกันมิให้ผู้ส่งหรือผู้รับข้อมูลปฏิเสธว่าตนไม่ได้ส่งหรือรับข้อมูลอิเล็กทรอนิกส์นั้น

รูปแบบของสิ่งหรือเครื่องหมายที่ใช้ระบุตัวบุคคลมี 3 ลักษณะ[3] คือ

1. สิ่งที่รู้ (something you know) หมายถึง วิธีการยืนยันตัวบุคคลซึ่งเฉพาะบุคคลที่ตรวจสอบและบุคคลที่ถูกตรวจสอบเท่านั้นที่รู้เกี่ยวกับสิ่งที่ใช้ตรวจสอบ เช่น การใช้รหัสผ่าน (password) รหัสประจำตัว (personal certification member: PIN) เป็นต้น

2. สิ่งที่มี (something you have) หมายถึง การที่บุคคลซึ่งถูกตรวจสอบมีสิ่งซึ่งใช้ยืนยันตัวบุคคล เช่น บัตรประจำตัวพนักงานในการบันทึกเวลาเข้า-ออกในการทำงานแต่ละวัน

---

[2]สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, พิมพ์ครั้งที่ 1 (กรุงเทพมหานคร: บริษัท จิรรัชการพิมพ์ จำกัด, 2545), น. 86-87.

[3]Benjamin Wright and Jane K. Winn, The Law of Electronic Commerce 3rd ed. (New York: Aspen Law & Business, 1988), pp. 3-10., อ้างใน สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, *อ้างแล้ว เชิงอรรถที่* 2, น. 85-86.

บัตรสมาร์ตการ์ด (smart card) บัตรแถบแม่เหล็ก (magnetic card) หรือลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) เป็นต้น

3. สิ่งที่เป็น (something you are) หมายถึง การใช้ลักษณะเฉพาะของตัวบุคคลในการตรวจสอบและพิสูจน์ตัวบุคคล สิ่งที่ใช้ตรวจสอบมักเป็นลักษณะทางชีวภาพของบุคคล เช่น ลายนิ้วมือ(fingerprints) ม่านตา(iris) เสียง(voice prints) หรือลักษณะของ DNA เป็นต้น

โดยเครื่องหมายที่ใช้ระบุตัวบุคคลแต่ละประเภทอาจถูกนำมาใช้ร่วมกันก็ได้เพื่อทำให้มีความปลอดภัยมากยิ่งขึ้น หากมีการใช้เพียงอย่างเดียว เรียกว่า ระบบรักษาความปลอดภัยแบบแฟคเตอร์เดี่ยว (one factor) เช่น รหัสผ่านซึ่งเป็นระบบพื้นฐานที่สุด แต่ถ้าใช้คู่กับบัตรอิเล็กทรอนิกส์ประเภทต่างๆเรียกว่า ระบบรักษาความปลอดภัยแบบแฟคเตอร์คู่ (two factor) เช่น รหัสประจำตัวและบัตรเอทีเอ็ม หรืออาจมีการนำรูปถ่ายมาติดลงไปด้วยก็เรียกว่า ระบบรักษาความปลอดภัยแบบ 3 แฟคเตอร์ (three factor) เช่น พาสปอร์ตอิเล็กทรอนิกส์ เป็นต้น[4]

ซึ่งจากรูปแบบของเครื่องหมายที่ใช้เพื่อระบุตัวบุคคลและประโยชน์ของการระบุตัวบุคคลที่เกี่ยวกับด้านการรักษาความปลอดภัยข้างต้น ส่งผลต่อการพัฒนาเทคโนโลยีที่ใช้ในการระบุตัวบุคคล ซึ่งอาจจะลำดับพัฒนาการของเทคโนโลยีสมัยใหม่ได้ 3 รูปแบบ[5] คือ

1. เทคโนโลยีบัตรแถบแม่เหล็ก (magnetic card) หรือบัตรสมาร์ตการ์ด (smart card) และรหัสข้อมูล ซึ่งการระบุตัวบุคคลโดยใช้เครื่องมือประเภทนี้ถูกพัฒนาขึ้นเพื่อให้เกิดความสะดวกแก่ผู้ใช้งานที่จะพกพา และสามารถใช้เข้าสู่ระบบฐานข้อมูลคอมพิวเตอร์ในลักษณะเป็นทางผ่านหรือเครื่องหมายแสดงถึงตัวบุคคลผู้มีสิทธิหรือได้รับอนุญาตจากผู้มีสิทธิ แต่มีข้อเสีย คือ สามารถถูกขโมยหรือถูกลักลอบไปใช้ในทางทุจริตได้ง่าย

2. เทคโนโลยีชีวภาพ (Biometrics) เป็นเทคโนโลยีที่อาศัยหลักการพื้นฐานของลักษณะทางชีวภาพของแต่ละบุคคลในการระบุตัวบุคคล โดยเทคโนโลยีชีวภาพจะแปลงลักษณะทางชีวภาพของบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ให้อยู่ในรูปข้อมูลดิจิตอลและคำนวณออกมาเพื่อเป็นค่าบันทึกความจำในลักษณะที่บ่งชี้ตัวบุคคลเจ้าของลักษณะทางชีวภาพนั้น

---

[4]ทศพล กนกนุวัตร์, How to Protect from Hackers, (กรุงเทพมหานคร: บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน), 2542), น. 46.

[5]สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, *อ้างแล้ว เชิงอรรถที่* 2, น. 87-90.

3. เทคโนโลยีการเข้ารหัสลับหรือวิทยาการการเข้ารหัสลับ (Cryptography) เป็นเทคโนโลยีที่พัฒนาขึ้นเพื่อใช้ในการรักษาความปลอดภัยของข้อมูลโดยใช้วิธีการและกระบวนการทางคณิตศาสตร์สร้างสิ่งที่มีอยู่ในรูปของตัวอักษร อักขระ ตัวเลข หรือสัญลักษณ์ใดๆขึ้นมา ซึ่งเรียกว่า "กุญแจ (Key)" และใช้กุญแจ (Key) ในการเข้ารหัสและถอดรหัสข้อมูล

2.2 ความหมายและลักษณะของเครื่องหมายที่ใช้ระบุตัวบุคคล

2.2.1 ความหมายของรหัสข้อมูล

รหัสข้อมูล คือ ตัวเลข ตัวอักษร หรือตัวเลขและตัวอักษรที่ใช้ร่วมกัน ซึ่งอาจจะมีจำนวนเท่าใดก็ได้ ที่ใช้เป็นเครื่องหมายที่ระบุถึงตัวบุคคลเพื่อเป็นสื่อกลางในการติดต่อทำธุรกรรมเข้าใช้ หรือเพื่อใช้เป็นรหัสผ่านเข้าถึงซึ่งข้อมูลที่ใช้ประกอบในการทำธุรกรรม

จากความหมายข้างต้นส่วนใหญ่รหัสข้อมูลจะประกอบด้วย 2 ส่วน คือ ชื่อผู้ใช้ (User name) เพื่อเป็นการบอกว่าเราคือใคร โดยการพิมพ์ชื่อตัวเราเพื่อเข้าสู่ระบบการใช้งานเครื่องคอมพิวเตอร์ และรหัสผ่าน (Password) ซึ่งจะใช้ร่วมกับชื่อผู้ใช้ในการพิสูจน์ยืนยันว่าเป็นบุคคลนั้นจริงๆ โดยเป็นส่วนที่คนอื่นไม่สามารถรับรู้ได้ และหากใช้จำนวนรหัสข้อมูลมากเท่าใดก็ยิ่งมีความปลอดภัยมากขึ้นเท่านั้น โดยที่เมื่อทดสอบโดยใช้เครื่องคอมพิวเตอร์ที่มีความเร็วในการประมวลผล 1,000,000 คำต่อวินาที ทำการถอดรหัสแล้วผลปรากฏดังตารางดังต่อไปนี้[6]

จำนวนตัวอักษร	การประกอบที่เกิดรหัสขึ้นได้	เวลาเฉลี่ยในการถอดรหัส
1	36	6 นาที
2	1,300	4 ชั่วโมง
3	47,000	5 วัน
4	1,700,000	6 เดือน
5	60,000,000	19 ปี
6	2,000,000,000	630 ปี

[6]Peter T. Davis และ Barry D. Lewis, Computer Security for Dummies, (กรุงเทพมหานคร: บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน), 2540), น. 155.

ดังนั้น รหัสข้อมูลจึงเป็นเครื่องหมายที่ช่วยในการรักษาความปลอดภัยด้วยการระบุสิทธิให้แก่ผู้ที่จะเข้ามายังระบบหรือเครือข่าย โดยรหัสผ่านที่ดีควรยาวเกินกว่า 5 ตัวอักษร เพราะถ้าสั้นเกินไปจะเดาง่ายและควรเป็นตัวหนังสือกับตัวเลขผสมกัน รหัสข้อมูลนี้ควรเก็บเป็นความลับและควรแก้ไขบ่อยๆด้วย สิ่งที่ไม่ควรนำมาใช้เป็นรหัสข้อมูลเนื่องจากง่ายต่อการสืบเสาะและหาได้อย่างรวดเร็ว ได้แก่ ชื่อขึ้นต้น ชื่อของบุคคล หมายเลขโทรศัพท์ วันเกิด หรือศัพท์ภาษาอังกฤษ เป็นต้น[7] โดยในชีวิตประจำวันของเราจะต้องเกี่ยวพันกับรหัสข้อมูลไม่ว่าในทางใดก็ทางหนึ่ง เช่น

1. <u>รหัสข้อมูลกับระบบตู้จดหมายอิเล็กทรอนิกส์</u> (Mailbox)

ซึ่งไปรษณีย์อิเล็กทรอนิกส์เป็นระบบที่ให้ผู้ใช้เครื่องคอมพิวเตอร์สามารถแลกเปลี่ยนข้อมูลกับผู้ใช้เครื่องคอมพิวเตอร์เครื่องอื่น(หรือกลุ่มผู้ใช้อื่น)บนเครือข่ายการติดต่อสื่อสารของผู้ให้บริการจดหมายอิเล็กทรอนิกส์ เช่น www.hotmail.com , www.yahoo.com , www.thaimail.com เป็นต้น ซึ่งผู้ให้บริการจะกำหนดชื่อผู้ใช้บริการ (E-mail address)[8] ซึ่งเปรียบเสมือนกับชื่อบุคคล เลขที่บ้าน และที่อยู่ที่จะใช้ในการรับส่งจดหมาย และรหัสผ่าน (password) เพื่อใช้ในการแสดงตัวบุคคลผู้เป็นเจ้าของ E-mail address ในการเข้าใช้บริการเปิดตู้จดหมาย (Mailbox)[9]

2. <u>รหัสข้อมูลกับการรักษาความปลอดภัย</u>

ด้วยคุณสมบัติเฉพาะตัวของรหัสข้อมูลที่ประกอบด้วยตัวเลขหรือตัวอักษรเพียงไม่กี่ตัวอักษร ทำให้มีความสะดวกในการจดจำแต่มีความยุ่งยากในการคาดเดาซึ่งรหัสข้อมูลดังกล่าวจึงทำให้มีการนำรหัสข้อมูลมาใช้ในการแสดงตัวบุคคลในระบบการรักษาความปลอดภัยมากขึ้น เช่น รหัสในการเข้าออกสถานที่ต่างๆ รหัสในการเปิด-ปิดตู้นิรภัย รวมทั้งรหัสในการเปิด-ปิดแฟ้มข้อมูลในระบบคอมพิวเตอร์ต่างๆ เป็นต้น

---

[7]ยืน ภู่สุวรรณ, <u>พจนานุกรมคอมพิวเตอร์และอินเตอร์เน็ต</u>, (กรุงเทพมหานคร: บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน), 2546), น. 328.

[8]E-mail address คือ ที่อยู่ประจำตัวของผู้ใช้ในระบบอินเตอร์เน็ตซึ่งใช้สำหรับการรับส่งไปรษณีย์อิเล็กทรอนิกส์ ซึ่งจะประกอบด้วย 3 ส่วน คือ ชื่อผู้ใช้ที่ส่งหรือรับข้อความ (Local name) , เครื่องหมาย@ และชื่อโดเมน (Domain name) ของเครื่องแม่ข่ายที่เราใช้บริการอยู่ เช่น somchai@hotmail.com เป็นต้น

[9]Mailbox คือ ตู้จดหมายอิเล็กทรอนิกส์หรือชื่อบัญชีในระบบไปรษณีย์อิเล็กทรอนิกส์หรือที่อยู่ที่ให้สามารถส่งข่าวสารไปยังผู้ที่อยู่ในคอมพิวเตอร์เครือข่าย ตู้จดหมายอิเล็กทรอนิกส์จะเก็บจดหมายอิเล็กทรอนิกส์ไว้เช่นเดียวกับตู้จดหมายหน้าบ้าน

3. <u>รหัสข้อมูลกับการให้บริการในระบบโทรศัพท์เคลื่อนที่</u>

ในการใช้บริการโทรศัพท์เคลื่อนที่ในระบบเติมเงิน (ระบบ pre-paid) นั้น ก่อนที่ผู้ใช้บริการจะสามารถใช้บริการโทรศัพท์ได้จะต้องมีการชำระค่าบริการโทรศัพท์ให้แก่ผู้ให้บริการล่วงหน้าผ่านระบบคอมพิวเตอร์หรือที่เรียกว่า "การเติมเงิน" เสียก่อน โดยผู้ใช้บริการจะต้องซื้อบัตรเติมเงินจากร้านค้าหรือร้านสะดวกซื้อต่างๆแล้วนำรหัสบัตรเติมเงินซึ่งประกอบด้วยตัวเลข 13 หลักหรือมากกว่านั้นที่ปรากฏอยู่บนบัตรเติมเงินทำการลงทะเบียนผ่านระบบเครือข่ายโทรศัพท์เคลื่อนที่เพื่อเติมเงินเข้าสู่ระบบของตน[10] ซึ่งระบบโทรศัพท์แบบเติมเงินในปัจจุบัน เช่น ระบบ one-two-call ระบบ happy D-prompt และระบบ just talk เป็นต้น

4. <u>รหัสข้อมูลที่ใช้ในการรับบริการอินเตอร์เน็ต หรือชั่วโมงอินเตอร์เน็ต</u>

เนื่องจากในการใช้บริการอินเตอร์เน็ตนั้น ผู้ใช้บริการโดยทั่วไปสามารถซื้อบริการเพื่อใช้เข้าสู่ระบบอินเตอร์เน็ตจากผู้ให้บริการ (Internet Service Provider: ISP)[11] ได้ในลักษณะของชั่วโมงอินเตอร์เน็ต ซึ่งจะมีราคาที่แตกต่างกันโดยขึ้นอยู่ระยะเวลาที่สามารถใช้บริการ ความเร็วในการเชื่อมต่อ และประสิทธิภาพในการใช้งาน โดยทั่วไปแล้วผู้ให้บริการก็จะกำหนดชื่อผู้ใช้บริการ (user name หรือ user ID) และรหัสผ่าน (password) ให้แก่ผู้ใช้บริการ เพื่อใช้แสดงตนในการเข้าสู่ระบบเครือข่ายอินเตอร์เน็ต จากนั้นระบบคอมพิวเตอร์จะทำการตรวจสอบชื่อผู้ใช้บริการและรหัสผ่านว่าเป็นผู้มีสิทธิหรือไม่เพื่อให้บริการต่อไป

5. <u>รหัสบัตรเอทีเอ็ม หรือ รหัสประจำตัว</u> (PIN : Personal Identification Number)

การที่ผู้เป็นเจ้าของบัญชีเงินฝากประสงค์จะขอใช้บริการฝากและถอนเงินผ่านเครื่องรับฝากถอนเงินอัตโนมัติ (Automatic Teller Machine หรือ ATM) นั้น จะต้องสมัครขอใช้บริการโดยเปิดบัญชีเงินฝากกับธนาคารก่อน จากนั้นธนาคารผู้ให้บริการจะออกบัตรเอทีเอ็มพร้อมรหัสประจำตัว (PIN : Personal Identification Number) ที่เป็นเลขรหัสเฉพาะตัวของเจ้าของบัญชีและเจ้าของบัตร โดยทั่วไปจะประกอบด้วยตัวเลขจำนวน 4 หลัก เพื่อใช้ประกอบการทำธุรกรรมต่างๆกับธนาคาร

---

[10]ขั้นตอนในการเติมเงินโดยใช้บัตรเติมเงินของบริษัทผู้ให้บริการต่างๆจะมีลักษณะที่คล้ายกัน คือ ผู้ใช้บริการต้องโทรศัพท์ไปยังหมายเลขพิเศษที่บริษัทผู้ให้บริการกำหนด แล้วทำการใส่หมายเลขบัตร หรือรหัสบัตร จากนั้นบริษัทผู้ให้บริการจะทำการเติมเงินให้โดยระบบอัตโนมัติ

[11]Internet Service Provider หรือ ISP คือ บริษัทหรือองค์กรผู้ให้บริการเชื่อมต่อเครือข่ายเข้าสู่อินเตอร์เน็ต ปัจจุบันประเทศไทยมีผู้ให้บริการรายใหญ่อยู่ 13 ราย

6. <u>รหัสข้อมูลกับลายมือชื่ออิเล็กทรอนิกส์</u> (Digital Signature)

เป็นการนำเทคโนโลยีการเข้ารหัสข้อมูลแบบกุญแจอสมมาตร (Asymmetric Key Cryptosystem) มาใช้ในการรักษาความปลอดภัยของข้อมูล โดยใช้ชุดของข้อมูลหรือที่เรียกว่า กุญแจ (key) มาใช้เป็นส่วนสำคัญในการสร้างลายมือชื่ออิเล็กทรอนิกส์หรือทั่วไปนิยมเรียกว่า "ลายมือชื่อดิจิทัล (Digital Signature)" เพื่อใช้ในการยืนยันตัวบุคคล ซึ่งขั้นตอนก็คือ การนำกุญแจส่วนตัว (Private key) ทำการเข้ารหัสข้อมูลที่ต้องการเพื่อเป็นการระบุถึงตัวผู้ส่งข้อมูลว่าเป็นใคร จากนั้นจึงใช้กุญแจอีกข้างหนึ่งที่เรียกว่า กุญแจสาธารณะ (Public key) ทำการถอดรหัสข้อมูล ซึ่งจะทำหน้าที่สำคัญในการตรวจสอบตัวบุคคลว่าเป็นเอกสารของผู้ส่งจริงหรือไม่ และมีการแก้ไขข้อมูลในระหว่างทางหรือไม่ ซึ่งเทคโนโลยีนี้ เรียกว่า เทคโนโลยี Public key Infrastructure หรือ PKI

2.2.2 <u>ความหมายของบัตรอิเล็กทรอนิกส์</u>

บัตรอิเล็กทรอนิกส์ คือ เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีการอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้ด้วยวิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า[12]

ซึ่งส่วนใหญ่บัตรอิเล็กทรอนิกส์จะประกอบด้วย 2 ส่วน คือ ส่วนที่เป็นบัตรซึ่งทำจากกระดาษหรือบัตรพลาสติกแข็งเพื่อทำหน้าที่รองรับส่วนที่เก็บข้อมูลซึ่งอาจทำให้ปรากฏความหมายด้วยลายลักษณ์อักษรหรือไม่ก็ได้ กับส่วนที่ทำหน้าที่ในการเก็บข้อมูลที่อยู่ในรูปสื่ออิเล็กทรอนิกส์ซึ่งเป็นส่วนที่สำคัญที่สุดเพื่อใช้ในการระบุตัวบุคคลของผู้ทรงสิทธิ ซึ่งสามารถจำแนกบัตรอิเล็กทรอนิกส์ตามวัสดุที่ใช้ในการเก็บรักษาข้อมูลได้ 3 ประเภท คือ

---

[12]ประมวลกฎหมายอาญา มาตรา 1(14)(ก) บัญญัติว่า "บัตรอิเล็กทรอนิกส์ หมายความว่า เอกสารหรือวัตถุอื่นใด ไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้ทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใดทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า"

2.2.2.1 Magnetic Stripe Card เป็นบัตรที่บันทึกข้อมูลในแถบแม่เหล็ก ได้แก่

1. บัตรเอทีเอ็ม และบัตรเดบิต (ATM Card, Debit Card) ธนาคารพาณิชย์ไทยได้เริ่มนำเครื่องรับฝากถอนเงินอัตโนมัติ (Automatic Teller Machine หรือ ATM) และบัตรเอทีเอ็ม (ATM Card) มาให้บริการแก่ประชาชนในปี พ.ศ. 2526 และเป็นที่นิยมอย่างแพร่หลายในปัจจุบัน เพราะทำให้การทำธุรกรรมต่างๆกับธนาคารทำได้ง่ายและสะดวกยิ่งขึ้นโดยเจ้าของบัญชีไม่จำต้องเดินทางไปสาขาของธนาคารที่ตนเองมีบัญชีอยู่แต่อย่างใด ต่อมาได้มีการพัฒนารูปแบบการให้บริการผ่านบัตรเอทีเอ็มมากขึ้น คือ จากเดิมที่ใช้เพียงเพื่อการถอนเงินสดจากเครื่องรับฝากถอนเงินอัตโนมัติให้สามารถใช้จ่ายแทนเงินสดได้อีกด้วย ซึ่งบัตรประเภทนี้เรียกว่า บัตรเดบิต (Debit Card) โดยทำรายการผ่านเครื่อง E.D.C (Electronic Data Capture)[13] จากนั้นธนาคารผู้ออกบัตรก็จะทำการหักเงินในบัญชีเงินฝากของเจ้าของบัตรทันทีพร้อมกับโอนไปยังบัญชีเงินฝากของร้านค้าผู้รับบัตร ซึ่งข้อมูลของธนาคารแห่งประเทศไทยระบุว่า ณ สิ้นปี พ.ศ. 2547 มีจำนวนบัตรเอทีเอ็มทั้งสิ้น 25,653,079 ใบ โดยมีการทำธุรกรรมโดยบัตรเอทีเอ็มผ่านเครื่องรับฝากถอนเงินอัตโนมัติประมาณ 2,122.30 พันล้านบาท หรือ 26% ของจีดีพี และกระทำธุรกรรมผ่านบัตรเดบิตถึง 1,417 พันล้านบาท[14]

---

[13]เครื่อง E.D.C (Electronic Data Capture) คือ เครื่องรับบัตรอัตโนมัติที่ธนาคารผู้ออกบัตรเครดิตติดตั้งที่ร้านค้าผู้รับบัตร เพื่อทำหน้าที่อนุมัติหรือปฏิเสธการใช้จ่ายผ่านบัตรเครดิตของผู้ถือบัตร เมื่อลูกค้ายื่นบัตรเครดิตเพื่อชำระราคาสินค้ากับทางร้าน พนักงานผู้รับบัตรจะนำบัตรด้านที่มีแถบแม่เหล็กรูดกับเครื่องเพื่อทำการอ่านรหัสในบัตร หากเป็นบัตรที่มีรหัสแม่เหล็กถูกต้องเครื่องก็จะทำการพิมพ์รายการซื้อขายพร้อมจำนวนเงินลงในใบบันทึกรายการขาย (Sales Slip) พร้อมทั้งขออนุมัติวงเงินทันทีโดยอัตโนมัติ ซึ่งใบบันทึกรายการขายจะถูกพิมพ์ออกมา 3 ฉบับเหมือนกัน โดยให้ผู้ถือบัตรลงลายมือชื่อในเอกสาร และร้านค้าจะมอบฉบับลูกค้าให้ผู้ถือบัตรไว้เป็นหลักฐาน ซึ่งเมื่อทำรายการแล้วธนาคารผู้ออกบัตรก็จะทำการโอนเงินเข้าบัญชีของร้านค้าต่อไป โดยร้านค้าไม่ต้องนำ Slip ไปขึ้นเงินกับธนาคารแต่อย่างใด ซึ่งหากมีการติดตั้งเครื่อง Pin Pad เพิ่มเข้าไปจะสามารถใช้กับบัตรเดบิต และ Stored Value Card ได้ด้วย อ้างใน ฝ่ายระบบการชำระเงิน ธนาคารแห่งประเทศไทย, ระบบการชำระเงินในประเทศไทย, (กรุงเทพมหานคร: บริษัท คาร์ลีโอเน่ อินเตอร์เนชั่นแนล จำกัด, สิงหาคม 2542), อภิธานศัพท์. น 4.

[14]กองบรรณาธิการ, "ระวังโจร ATM ฉกรหัสคาตู้," วารสารการเงินการธนาคาร, ฉบับที่ 282 (ตุลาคม 2548), น. 216.

2. บัตรเครดิต (Credit Card) ตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 มาตรา 3 ได้ให้คำนิยามของ บัตรเครดิต หมายความว่า บัตร หรือสิ่งอื่นใดที่ผู้ประกอบการออกให้แก่ลูกค้าเพื่อใช้ชำระค่าสินค้า บริการ หรือค่าอื่นใด แทนการชำระด้วยเงินสด หรือเพื่อใช้เบิกถอนเงินสด โดยลูกค้าจะต้องชำระค่าธรรมเนียม ค่าบริการ ดอกเบี้ย หรือค่าอื่นใด แต่ไม่รวมถึงบัตรที่ได้มีการชำระค่าสินค้า ค่าบริการ หรือค่าอื่นใดไว้ล่วงหน้าแล้ว[15] ดังนั้น บัตรเครดิตจึงเป็นเครื่องมือในการชำระค่าสินค้าที่ทำให้ผู้ถือบัตรสามารถได้สินค้าและค่าบริการจากร้านค้าอันเนื่องมาจากการเตรียมการของธนาคารหรือบริษัทผู้ออกบัตรที่ตกลงรับชำระเงินค่าสินค้าและบริการให้แก่ลูกค้า โดยผู้ถือบัตรมีหน้าที่ในการชำระเงินแก่ธนาคารหรือบริษัทผู้ออกบัตรตามเงื่อนไขที่ตกลงไว้ และบางกรณีบัตรเครดิตสามารถนำไปเบิกเงินสดได้ด้วย[16] โดยมีคู่สัญญาที่เกี่ยวข้อง 3 ฝ่าย คือ ธนาคารหรือบริษัทผู้ออกบัตร ซึ่งจะเป็นธนาคารพาณิชย์หรือบริษัทผู้ประกอบกิจการให้บริการบัตรเครดิต[17] อีกฝ่ายหนึ่งที่เรียกว่า สมาชิกบัตรหรือผู้ถือบัตร และอีกกลุ่มคนอีกกลุ่มหนึ่งที่เรียกว่า ผู้รับบัตร ซึ่งก็คือ ร้านค้า โรงแรม และสถานบริการต่างๆที่มีข้อตกลงกับธนาคารหรือบริษัทผู้ออกบัตรว่ายินยอมรับบัตรเครดิตแทนการใช้เงินสดจากลูกค้าเพื่อแลกกับสินค้าและบริการ นอกจากนั้น ยังมีการชำระราคาค่าสินค้าและบริการด้วยบัตรเครดิตผ่านระบบเครือข่ายอินเตอร์เน็ต โดยการกรอกหมายเลขบัตรเครดิตลงในแบบฟอร์มการชำระเงินที่กำหนด

3. บัตรประจำตัวนักศึกษา คือ บัตรอิเล็กทรอนิกส์ที่สถาบันการศึกษาออกให้แก่นักศึกษาเพื่อใช้เป็นเครื่องหมายแสดงตัวในการติดต่อเพื่อทำกิจธุระต่างๆกับสถาบันการศึกษา ได้แก่ การชำระค่าเล่าเรียนผ่านบัตร การใช้บัตรเพื่อเข้าออกสถานศึกษา รวมถึงการใช้บริการต่างๆของมหาวิทยาลัย เช่น บริการห้องสมุดเพื่อยืมและคืนหนังสือ เป็นต้น

4. บัตรประจำตัวพนักงาน คือ บัตรอิเล็กทรอนิกส์ที่บริษัทนำมาใช้เป็นเครื่องหมายแสดงตัวบุคคล ผู้ซึ่งเป็นพนักงานของบริษัทและเพื่อประโยชน์ในด้านต่างๆ เช่น ใช้ลงเวลาทำงานแทนระบบเดิมที่กำหนดให้พนักงานต้องเขียนเวลาทำงานลงสมุดบันทึกเวลาทำงาน ใช้ในการทำ

---

[15]โปรดดู พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 มาตรา 3

[16]Drury, T. and Ferrier C.W., Credit Card (London: Billing & Son Limited, 1984), p. XII- 5. อ้างใน สุรเชษฐ์ ชีรวินิจ, กฎหมายบัตรเครดิต (Law on credit card), เอกสารประกอบการเรียนการสอน กองบัญชาการวิชาการ โรงเรียนนายร้อยตำรวจ ปีการศึกษา พ.ศ.2544, น. 3.

[17]บริษัทบัตรเครดิตที่สำคัญ เช่น Visa , Master Card , Diners และ American Express เป็นต้น

รายการลาหยุดผ่านระบบคอมพิวเตอร์ของบริษัท หรือใช้เป็นบัตรผ่านเข้าและออกสถานที่ทำงาน เพื่อเป็นการรักษาความปลอดภัยในสถานที่ทำงาน เป็นต้น

5. บัตรคูปองอาหาร คือ บัตรอิเล็กทรอนิกส์ชนิดหนึ่งที่ศูนย์อาหารของห้างสรรพสินค้าต่างๆนิยมนำเข้ามาใช้เป็นสื่อกลางในการซื้อขายอาหารแทนเงินสดและคูปองอาหารที่ทำด้วยกระดาษแบบเดิม เพียงแต่ผู้ซื้อทำการรูดบัตรคูปองอาหารผ่านเครื่องบันทึกรายการ เครื่องก็จะทำการตรวจสอบยอดเงินคงเหลือในบัตรแล้วจะทำการหักลบมูลค่าเงินตามราคาค่าอาหารที่กำหนดไว้แทนการชำระเงิน และจะหักลบวงเงินลงเรื่อยๆเมื่อมีการใช้บัตรจนกว่าวงเงินที่กำหนดไว้จะหมด

2.2.2.2 Integrated Circuit Chip Card หรือเรียกอีกอย่างว่าบัตรสมาร์ตการ์ด คือ บัตรพลาสติกที่มีวงจรอิเล็กทรอนิกส์ (Integrated Circuit) หรือที่เรียกว่าไมโครชิพฝังอยู่ ซึ่งไมโครชิพดังกล่าวมีหน่วยความจำและหน่วยประมวลผลทำหน้าที่ในการอ่านและคำนวณผลรวมทั้งสามารถบันทึกข้อมูลลงได้ เช่น บัตรโทรศัพท์ บัตรเงินสด และบัตรสุขภาพ เป็นต้น และถือเป็นบัตรที่ทันสมัยที่สุดในปัจจุบัน ซึ่งสามารถแบ่งประเภทของชิพที่ใช้ในบัตรสมาร์ตการ์ดได้[18] ดังนี้

1. สมาร์ตการ์ดชนิด Memory card หรืออีกชื่อหนึ่ง เรียกว่า Synchronous card เช่น บัตรโทรศัพท์แบบ TOT ซึ่งภายในบัตรจะเก็บข้อมูลในลักษณะของจำนวนนับ (Counter) โดยจำนวนนับนี้จะเป็นตัวเลขแทนมูลค่าของเงินที่ระบุบนบัตร การนับเลขเป็นการนับถอยหลังเพื่อเป็นการนับมูลค่าที่คงเหลือในบัตร คือ หากใช้บัตรในการโทรศัพท์ไปเรื่อยๆมูลค่าในบัตรก็จะถูกลดลงตามไปด้วย

2. สมาร์ตการ์ดชนิด Processor card ซึ่งเป็นสมาร์ตการ์ดที่ได้รับการปรับปรุงมาจากสมาร์ตการ์ดชนิด Memory card ด้วยการใส่เทคโนโลยีไมโครโปรเซสเซอร์เข้าไปในชิพ เพื่อทำให้ชิพสามารถทำการประมวลผลข้อมูลได้และเพิ่มความปลอดภัยให้แก่ข้อมูลให้สูงขึ้น เช่น ซิมการ์ดในโทรศัพท์มือถือ เป็นต้น

จะเห็นได้ว่าในปัจจุบันได้มีการนำเทคโนโลยีที่เกี่ยวกับสมาร์ตการ์ดมาใช้อย่างแพร่หลายเพราะในชิพสามารถเก็บข้อมูลได้ในจำนวนที่มากทำให้เกิดความสะดวกที่จะใช้บัตรเพียงใบเดียวในการเก็บรักษาข้อมูลที่สำคัญต่างๆ ซึ่งประเทศไทยก็กำลังที่จะนำบัตรสมาร์ตการ์ด

---

[18]ขนิษฐา จิตรหลัง, "สมาร์ตการ์ด (Smart Card),", น. 10-12. <www.student.chula.ac.th/~46801073/SM.pdf>

มาใช้เพื่อทำเป็นบัตรประจำตัวประชาชนโดยนำข้อมูลของบุคคลในด้านต่างๆมาบรรจุไว้ภายในบัตร เช่น ข้อมูลเกี่ยวกับทะเบียนราษฎร ข้อมูลเกี่ยวกับสิทธิประกันสังคม ข้อมูลเกี่ยวกับสิทธิประกันสุขภาพ ข้อมูลเกี่ยวกับการได้รับการยกเว้นค่ารักษาพยาบาล ข้อมูลเกี่ยวกับภาษี ข้อมูลเกี่ยวกับข้าราชการ และข้อมูลเกี่ยวกับครอบครัวเกษตรกร เป็นต้น

2.2.2.3 Full Face Magnetic Card เป็นบัตรที่บันทึกข้อมูลในแถบบันทึกข้อมูลที่มีลักษณะเป็นเส้นบางเล็กอยู่ด้านหลังบัตร ซึ่งมักจะใช้ประโยชน์ในลักษณะเป็นบัตรที่ผู้ถือบัตรได้จ่ายเงินหรือค่าบริการล่วงหน้า (Pay Before) ให้แก่บริษัทผู้ออกบัตร เพื่อใช้ชำระค่าสินค้าหรือบริการที่มีมูลค่าน้อย เช่น บัตรโทรศัพท์สาธารณะ บัตรที่จอดรถ บัตรทางด่วน เป็นต้น เมื่อผู้ถือบัตรใช้บัตรเพื่อชำระค่าสินค้าและบริการแล้วมูลค่าเงินในบัตรจะลดลงเรื่อยๆตามการใช้จนกระทั่งหมดมูลค่า

2.2.3 ลักษณะทางชีวภาพที่ใช้ระบุตัวบุคคล (Biometrics)

เป็นระบบที่ใช้แสดงตัวบุคคลโดยอาศัยลักษณะจำเพาะทางกายภาพของแต่ละบุคคลเป็นเครื่องจำแนกสิทธิ โดยมีหลักการพื้นฐานที่ว่า มนุษย์ทุกคนจะมีรูปร่าง ลักษณะนิสัย และลักษณะทางกายภาพที่มีอยู่เพียงหนึ่งเดียวไม่มีทางที่จะเหมือนกับบุคคลอื่นได้ แม้แต่ฝาแฝดที่เกิดจากไข่ใบเดียวกันก็ตาม (Identical twins) ซึ่งลักษณะของไบโอเมทริคที่มีใช้อยู่ในปัจจุบันได้แก่ ลายนิ้วมือ ลายมือชื่อ รอยฝ่ามือ รูปแบบของม่านตา รูปแบบของคลื่นเสียง รอยฝีปาก คลื่นสมอง รูปทรงเลขาคณิตของใบหน้า เป็นต้น เมื่อมีการใช้ไบโอเมทริคโดยผู้ทรงสิทธิแล้วเครื่องมือก็จะรับรู้ข้อมูลนั้นแล้วเปลี่ยนสัญญาณอนาล็อกที่ได้รับมาให้เป็นสัญญาณดิจิตอล จากนั้นจึงนำไปเปรียบเทียบกับฐานข้อมูลที่บันทึกไว้ เช่น

1. การตรวจสอบลักษณะม่านตา คือ จะใช้ขนาด ตำแหน่ง และรูปแบบของการวางตัวของเส้นเลือดเป็นตัวตัดสิน แต่มิใช่ว่าจะใช้ภาพถ่ายหรือรูปภาพที่มีการบันทึกเป็นตัวตรวจสอบโดยตรง หากวัดจากความหนาแน่นของแสงอินฟราเรดที่สะท้อนออกมาจากตำแหน่งต่างๆกัน โดยข้อมูลที่ได้นี้จะเป็นข้อมูลดิจิตอลที่บ่งบอกถึงลักษณะการวางตัวของเส้นเลือดในม่านตา หากมีลักษณะที่ถูกต้องตรงกับข้อมูลที่บันทึกไว้ก็จะแสดงว่าเป็นผู้ทรงสิทธิ

2. การตรวจสอบลายพิมพ์นิ้วมือ คือ การตรวจสอบลักษณะทางกายภาพของนิ้วมือ เช่น เส้นโค้ง รอยยัก และเส้นนูน เป็นเครื่องตัดสิน โดยหลังจากที่ผู้ใช้วางนิ้วมือลงบนแผ่นแก้วก็จะ

มีการส่องแสงออกมาจากภายในตัวเครื่อง เมื่อแสงถูกนิ้วมือก็จะสะท้อนกลับมายังเครื่องสแกน เพื่อตรวจสอบว่าเหมือนกับผู้ทรงสิทธิหรือไม่

3. การตรวจสอบรอยฝ่ามือ คือ เป็นกระบวนการที่ใช้ลักษณะทางเรขาคณิตของฝ่ามือ ความยาวของนิ้ว และความโปร่งแสงของผิวหนัง มาเป็นปัจจัยในการตรวจสอบ โดยวางฝ่ามือลงบนแผ่นแก้วที่มีลักษณะเป็นร่องตามลักษณะกายวิภาคศาสตร์ของนิ้วมือแล้วเครื่องอ่านจะสแกนฝ่ามือพร้อมกับบันทึกความหนาแน่นของลำแสงจากหลอดไฟเพื่อเปรียบเทียบกับข้อมูลดิจิตอลของผู้ทรงสิทธิ

4. การตรวจสอบคลื่นเสียง คือ การอาศัยเสียงและการสะท้อนของเสียงเป็นเครื่องชี้วัด โดยผู้ใช้จะต้องพูดวลีที่กำหนดเข้าไปในเครื่อง จากนั้นเครื่องจะแปลงคลื่นเสียงให้อยู่ในรูปความถี่และวิเคราะห์ถึงการกระจายความถี่เพื่อเปรียบเทียบกับข้อมูลดิจิตอลของผู้ทรงสิทธิ[19]

จะเห็นได้ว่าเทคโนโลยีชีวภาพที่ใช้ระบุตัวบุคคล (Biometrics) จึงเป็นเครื่องมือวัด (measurement) ที่พิจารณาจากลักษณะทางกายภาพประจำตัวของแต่ละบุคคล (physical Attribure) หรือจากลักษณะการกระทำของแต่ละบุคคล (physical Activity) เนื่องจากลักษณะดังกล่าวจะมีลักษณะเฉพาะที่แตกต่างกันไปในแต่ละบุคคลและมีลักษณะที่เป็นหนึ่งเดียว โดยการนำลักษณะเฉพาะตัวดังกล่าวมาเทียบเคียงกับฐานข้อมูลที่เก็บเอาไว้ ซึ่งระบบตรวจสอบมีหลายระบบ เช่น การใช้ระบบ AFIS (automated fingerprint identification system) เป็นต้น ดังนั้น จึงทำให้ผู้มีสิทธิเข้าใช้บริการโดยผ่านระบบไบโอเมทริคมีได้เพียงคนเดียว และทำให้ปัญหาในลักษณะที่เป็นการสูญหาย ถูกลัก หรือการปฏิเสธการรับบัตรอิเล็กทรอนิกส์หมดสิ้นไป อีกทั้ง การกระทำความผิดในลักษณะการปลอมแปลงก็จะลดลงเนื่องจากกลุ่มคนร้ายต้องมีความสามารถพิเศษในการจัดหาข้อมูลเฉพาะบุคคลดังกล่าว สำหรับในการนำเทคโนโลยีดังกล่าวมาใช้กับการทำธุรกรรมทางการเงินนั้นจะมีการนำมาใช้ควบคู่กับการใช้บัตรอิเล็กทรอนิกส์เพื่อให้มีความปลอดภัยมากยิ่งขึ้น แต่เทคโนโลยีดังกล่าวก็มีข้อเสียที่ว่ามีค่าใช้จ่ายสูง มีขนาดใหญ่ และระดับความน่าเชื่อถือในอุปกรณ์ที่รับข้อมูล จึงทำให้มีการนำไปในเชิงธุรกิจน้อยมาก และถูกนำไปใช้ในการควบคุมการเข้าถึงหรือให้สิทธิในการใช้โปแกรมของรัฐบาลเท่านั้น[20]

---

[19]*ทศพล กนกนุวัตร์, อ้างแล้ว เชิงอรรถที่* 4, น. 61-66.

[20]Jerry Iannacci, Ron Morris, access device Fraud and Related Financial Crimes (CRS Press LLC, 2000), pp. 46-48.

ดังนั้น จะเห็นได้ว่าเครื่องหมายที่ใช้ระบุตัวบุคคลประเภทต่างๆ ไม่ว่าจะเป็น รหัสข้อมูลบัตรอิเล็กทรอนิกส์ หรือไบโอเมทริค ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ต่างมีจุดร่วมกัน คือ สิ่งที่สื่อความหมายมิใช่ลักษณะตัวอักษร ตัวเลข หรือลักษณะทางชีวภาพที่ปรากฏและรับรู้ได้ด้วยตาเปล่า แต่แท้จริงแล้วสิ่งที่เป็นเครื่องหมายที่ใช้ระบุตัวบุคคลมีลักษณะเป็นสัญลักษณ์ที่อยู่ในลักษณะของภาษาคอมพิวเตอร์ การใช้เครื่องหมายที่ใช้ระบุตัวบุคคลประเภทต่างๆจึงต้องแปลงสิ่งที่เราสามารถมองเห็นทั่วไปให้อยู่ในลักษณะภาษาที่เครื่องคอมพิวเตอร์สามารถรับรู้และประมวลผลได้ที่เรียกว่า "ข้อมูลอิเล็กทรอนิกส์หรือข้อมูลดิจิตอล" ซึ่งเป็นภาษาของเครื่องโดยจะอยู่ในระบบเลขฐานสองที่ประกอบด้วยตัวเลข 2 ตัว ได้แก่ 0 และ 1 โดยเลขแต่ละตัวจะมีหน่วยเป็นบิต (Binary digit : bit) เช่น 001 จะมี 3 บิต แต่ถ้ารวมกันได้ 8 ตัว จะเรียกว่าไบต์ (Byte) ซึ่งบิตเพียงบิตเดียวยังไม่สามารถแทนข้อมูลใดๆได้จะต้องนำบิตมารวมกันเข้า เช่น 8 บิต 16 บิต 32 บิต 64 บิต หรือ 128 บิต เป็นต้น เพื่อใช้แต่ละไบต์แทนข้อมูลต่างๆไม่ว่าจะเป็นตัวเลขหรือตัวอักษร หรือสัญลักษณ์พิเศษที่เรารับรู้กันหนึ่งตัว (character) เช่น ตัวอักษร ก คือ 1000 0000 หรือเลข 5 คือ 0000 0101 เป็นต้น[21] จึงทำให้ตัวอักษรหรือตัวเลขของเครื่องหมายที่ใช้ระบุตัวบุคคลประเภทต่างๆที่เราเห็นผ่านเครื่องคอมพิวเตอร์มิใช่ตัวอักษรหรือตัวเลขที่เราเข้าใจแต่เป็นภาษาของเครื่องคอมพิวเตอร์ที่อยู่ในลักษณะของ 0 และ 1 นั่นเอง

2.3 ลักษณะการกระทำความผิด

ลักษณะของการกระทำความผิดอาจจะเกิดขึ้นได้หลายรูปแบบที่เกี่ยวเนื่องกับขั้นตอนต่างๆในกระบวนการของเครื่องหมายที่ใช้ระบุตัวบุคคล ไม่ว่าจะในขั้นตอนการสมัครเพื่อขอใช้บริการ ขั้นตอนการส่งมอบ และขั้นตอนของการนำเครื่องหมายที่ใช้ระบุตัวบุคคลไปใช้ซึ่งอาจจะกระทำทุจริตโดยผู้มีสิทธิหรือโดยกลุ่มคนร้ายก็ได้ ซึ่งสามารถแบ่งรูปแบบการกระทำความผิดได้ออกเป็น 6 รูปแบบ คือ

---

[21]กิตติ ภักดีวัฒนะกุล, คัมภีร์ระบบสารสนเทศ (Information System),(กรุงเทพมหานคร: บริษัท เคพีที คอมพ์ แอนด์ คอนซัลท์ จำกัด , 2546), น. 223.

2.3.1 การใช้ข้อมูลปลอมในการสมัครใช้บริการ (Fraudulent Application)

กลุ่มคนร้ายที่ประสงค์จะสมัครขอใช้บริการบริการอาจนำข้อมูลที่เป็นเท็จหรือแอบอ้างนำข้อมูลส่วนบุคคลของบุคคลอื่นกรอกลงในแบบคำขอใช้แทนข้อมูลของตน ซึ่งข้อมูลส่วนบุคคลต่างๆไม่ว่าจะเป็นหมายเลขบัตรประจำตัวประชาชน ชื่อ-นามสกุล และที่อยู่นั้น กลุ่มคนร้ายสามารถหาได้จากการรับซื้อสำเนาบัตรประจำตัวประชาชนที่เจ้าของบัตรทำหายจากร้านถ่ายเอกสาร หรือจากบริษัทห้างร้านต่างๆที่เจ้าของบัตรนำไปใช้เป็นหลักฐานประกอบการสมัครงานก็ได้ โดยการกระทำดังกล่าวย่อมจะสร้างความเสียหายให้แก่ผู้เป็นเจ้าของข้อมูลและบริษัทผู้ให้บริการอย่างมาก เช่น กลุ่มคนร้ายนำข้อมูลส่วนบุคคลที่รับซื้อมาและปลอมแปลงข้อมูลของผู้อื่นเพื่อขอจดทะเบียนเช่าใช้บริการโทรศัพท์เคลื่อนที่ในระบบเหมาจ่ายรายเดือน (Post-paid) และนำซิมการ์ดโทรศัพท์ที่ได้ไปใช้แสวงหาประโยชน์โดยลักลอบให้บริการโทรศัพท์ระหว่างประเทศ ส่งผลให้บริษัทผู้ให้บริการต่างๆและบริษัท โทรคมนาคมไทย จำกัด (มหาชน) หรือการสื่อสารแห่งประเทศไทย (เดิม) ในฐานะผู้ให้บริการโทรศัพท์ระหว่างประเทศได้รับความเสียหายเนื่องจากเรียกเก็บค่าใช้บริการไม่ได้เป็นจำนวนรวมกันปีละหลายร้อยล้านบาท

หรือกรณีการสมัครขอใช้บริการบัตรเครดิต กลุ่มคนร้ายก็ใช้วิธีการหลอกลวงพนักงานของธนาคารหรือบริษัทผู้ออกบัตรด้วยการปลอมแปลงบัตรประจำตัวประชาชนหรือสำเนาทะเบียนบ้านของบุคคลใดบุคคลหนึ่ง จากนั้นก็จะไปเช่าบ้านพักอาศัยและแจ้งสถานที่นั้นเป็นที่อยู่อาศัยในคำขอใช้บริการ เมื่อมีการอนุมัติบัตรแล้ว กลุ่มคนร้ายจะนำบัตรประชาชนปลอมไปรับบัตรเครดิตกับพนักงานของธนาคารหรือบริษัทผู้ออกบัตร เมื่อได้รับบัตรเครดิตแล้วก็จะนำบัตรไปใช้ในการซื้อสินค้าหรือบริการได้เหมือนกับบัตรที่แท้จริง เพราะเป็นบัตรที่ออกมาให้แก่ผู้ขอใช้บริการจริง จนกระทั่งเมื่อธนาคารหรือบริษัทผู้ออกบัตรไม่สามารถเรียกเก็บเงินจากเจ้าของบัตรที่แท้จริงซึ่งถูกแอบอ้างได้แล้ว จึงรู้ว่าถูกหลอกและอายัดบัตร ซึ่งคนร้ายก็สามารถนำบัตรที่ถูกอายัดไปใช้กระทำความผิดอื่นๆได้อีก เช่น การแปลงข้อมูลบนหน้าบัตร เป็นต้น[22]

สำหรับการปลอมเอกสารของผู้อื่นเพื่อขอใช้บัตรเอทีเอ็มนั้น เป็นรูปแบบของอาชญากรรมที่ไม่ค่อยพบมากนัก เพราะขั้นตอนการสมัครขอใช้บริการบัตรเอทีเอ็มนั้นผู้ขอใช้

---

[22]สุรเชษฐ์ ชีววินิจ, กฎหมายบัตรเครดิต (Law on credit card), เอกสารประกอบการเรียนการสอน กองบัญชาการวิชาการ โรงเรียนนายร้อยตำรวจ ปีการศึกษา พ.ศ.2544, น. 12-13.

จะต้องมีบัญชีเงินฝากกับธนาคารผู้ให้บริการและใช้บริการถอนเงินได้เฉพาะเงินฝากที่คงเหลืออยู่ในบัญชีเท่านั้น จึงไม่มีประโยชน์ที่คนร้ายจะได้รับจากปลอมเอกสารดังกล่าว

2.3.2 <u>การขโมยหรือลักลอบใช้รหัสข้อมูลและบัตรอิเล็กทรอนิกส์</u>

โดยปกติรหัสข้อมูลบริษัทผู้ให้บริการจะทำการบันทึกรหัสข้อมูลไว้ในวัสดุในรูปแบบต่างๆเพื่อความสะดวกในการส่งมอบให้ผู้ใช้บริการ เช่น รหัสบัตรเอทีเอ็มก็จะถูกบันทึกไว้บนกระดาษและบรรจุไว้ในซองพร้อมกับบัตรเอทีเอ็มเพื่อรอส่งมอบให้แก่ลูกค้า หรือชั่วโมงอินเตอร์เน็ตผู้ให้บริการจะกำหนดชื่อผู้ใช้บริการและรหัสผ่านไว้ในซองเพื่อจำหน่ายให้แก่ลูกค้า เป็นต้น ซึ่งกลุ่มคนร้ายจะทำการขโมยซึ่งวัสดุที่บันทึกรหัสข้อมูลหรือบัตรอิเล็กทรอนิกส์ที่เก็บรักษาไว้ที่บริษัทผู้ให้บริการหรือที่อยู่กับผู้เป็นเจ้าของหรือผู้ที่มีสิทธิใช้ ซึ่งลักษณะการขโมยรหัสข้อมูลหรือบัตรอิเล็กทรอนิกส์นั้นจะมีอยู่ 2 ลักษณะ คือ

1. การขโมยรหัสข้อมูลหรือบัตรอิเล็กทรอนิกส์ก่อนที่จะถึงมือของผู้ขอใช้บริการซึ่งจะมีอยู่ 2 ขั้นตอน คือ

ขั้นตอนที่ 1 เมื่อบริษัทผู้ให้บริการทำการบันทึกรหัสข้อมูลลงในกระดาษหรือวัสดุบันทึกอื่นๆ หรือได้ออกบัตรอิเล็กทรอนิกส์ให้แก่ลูกค้าแล้วและเก็บรักษาไว้เพื่อรอส่งมอบหรือจำหน่ายให้แก่ลูกค้า พนักงานของบริษัทผู้ให้บริการอาจจะขโมยรหัสข้อมูลหรือบัตรอิเล็กทรอนิกส์ที่เตรียมไว้นำไปใช้เป็นประโยชน์ส่วนตัว เช่น การขโมยบัตรเอทีเอ็มพร้อมรหัสประจำตัวโดยพนักงานธนาคาร การขโมยบัตรเครดิตโดยพนักงานของธนาคาร หรือการที่พนักงานของบริษัทผู้ให้บริการโทรศัพท์เคลื่อนที่ขโมยบัตรเติมเงินเพื่อนำไปขายให้แก่บุคคลภายนอก เป็นต้น

ขั้นตอนที่ 2 มักจะเกิดขึ้นระหว่างการส่งรหัสข้อมูลหรือบัตรอิเล็กทรอนิกส์ไปให้แก่ลูกค้าโดยทางไปรษณีย์ไปยังสถานที่ทำงานหรือสถานที่ที่อยู่ของผู้ขอใช้บริการ โดยบุรุษไปรษณีย์หรือพนักงานในสถานที่ทำงานของผู้รับอาจจะขโมยรหัสข้อมูลหรือบัตรอิเล็กทรอนิกส์นั้นนำไปใช้เป็นประโยชน์ส่วนตัว เช่น การขโมยบัตรเครดิตโดยบุรุษไปรษณีย์ ซึ่งวิธีการนี้คนที่ขโมยเอาไปจะเซ็นชื่อในช่องลายมือชื่อของผู้ถือบัตรจึงทำให้บัตรนี้สามารถใช้ได้เหมือนเป็นของเจ้าของที่แท้จริงจนกระทั่งเมื่อครบกำหนดงวดชำระเงิน (รอบบัญชีซึ่งปกติก็จะทุกๆสิ้นเดือน) ที่ธนาคารหรือบริษัทผู้ออกบัตรเรียกเก็บเงินจากผู้ถือบัตร ผู้ขอใช้บัตรก็จะปฏิเสธและร้องเรียนไปยังธนาคารหรือบริษัทผู้ออกบัตรว่ายังไม่เคยได้รับบัตรเลยก็จะทำให้บัตรที่ถูกขโมยถูกระงับการใช้ ซึ่งกลุ่มคนร้ายก็จะไม่นำบัตรนั้นออกมาใช้อีกเนื่องจากเสี่ยงที่จะถูกจับกุม ในปัจจุบันธนาคารหรือบริษัทผู้ออกบัตรมีวิธีป้องกันโดยการล็อครหัสไว้ไม่ให้ใช้จนกว่าผู้ถือบัตรได้รับบัตรและโทรศัพท์กลับไปที่ธนาคารหรือ

บริษัทผู้ออกบัตรโดยแจ้งข้อมูลส่วนตัวในการยืนยันตัวบุคคลเพื่อปลดรหัสล็อค จึงจะสามารถใช้บริการบัตรเครดิตนั้นได้

2. การขโมยหรือเก็บกระดาษที่บันทึกรหัสข้อมูลหรือบัตรอิเล็กทรอนิกส์ที่อยู่ในการครอบครองของผู้ที่มีสิทธิใช้ที่ลืมทิ้งไว้หรือทำสูญหายไปใช้ โดยผู้ที่เก็บได้จะนำไปแสดงตัวว่าเป็นผู้มีชื่อตามบัตรหรือมีสิทธิใช้บัตรดังกล่าว เช่น กรณีของบัตรเครดิตที่กลุ่มคนร้ายจะนำบัตรที่ลักมาหรือเก็บตกมาได้ไปใช้กับร้านค้าพร้อมลงลายมือชื่อใน Sales Slip เป็นชื่อเจ้าของบัตร ซึ่งการขโมยนี้อาจจะกระทำโดยการล้วงกระเป๋า การขโมยจากล็อคเกอร์ในสนามกอล์ฟ โรงแรม สถานที่ออกกำลังกายต่างๆ หรือ เกสท์เฮาส์ และจะเป็นการขโมยที่แนบเนียนมากเพราะกลุ่มคนร้ายเหล่านี้มักจะไม่แตะต้องเงินทองหรือของมีค่าในกระเป๋าแต่จะเอาเฉพาะบัตรเครดิตเท่านั้น หากผู้เสียหายมีบัตรหลายใบในกระเป๋าและพวกกลุ่มคนร้ายหยิบไปเพียงใบเดียวแล้วเหยื่อก็ไม่อาจจะรู้ได้ หรือมิฉะนั้นกลุ่มคนร้ายก็อาจจะเอาบัตรที่หมดอายุแล้วและเป็นของคนอื่นที่ขโมยมาเอาใส่ไว้แทนในกระเป๋า กว่าผู้เสียหายจะรู้ก็เมื่อนำบัตรเครดิตไปใช้หรือได้รับแจ้งยอดหนี้ค่าใช้บริการจากธนาคารหรือบริษัทผู้ออกบัตร ซึ่งกรณีเช่นนี้ธนาคารหรือบริษัทผู้ออกบัตรจะไม่รับผิดชอบให้เพราะถือว่าไม่ได้มีการแจ้งอายัดหรือแจ้งบัตรหายไว้ก่อน จึงทำให้ผู้ถือบัตรต้องรับผิดชอบสำหรับจำนวนเงินที่ถูกขโมยใช้ไป[23] หรืออาศัยโอกาสที่เป็นคนใกล้ชิดกับผู้เป็นเจ้าของบัตรเอทีเอ็มจนทราบรหัสประจำตัว (PIN : Personal Identification Number) และแอบนำบัตรจากเจ้าของไปกดเงิน หรือกรณีที่คนร้ายนำเศษวัสดุ เช่น ไม้จิ้มฟัน หมากฝรั่ง หรือกระดาษทิชชูไปปิดกั้นไว้ที่ช่องรับเงิน เมื่อผู้เป็นเจ้าของบัตรกดรหัสเรียบร้อยแล้วเงินจะตกค้างอยู่ในช่องรับเงินพร้อมกับบัตรเอทีเอ็มก็จะไม่คืนออกมาจากเครื่อง เนื่องจากเครื่องทำงานไม่ครบวงจร จากนั้นกลุ่มคนร้ายจะหลอกลวงว่าหากกดรหัสอีกครั้งบัตรเอทีเอ็มอาจจะออกมาก็ได้ เมื่อเจ้าของบัตรกดรหัสอีกครั้งคนร้ายจะแอบดูและจดจำรหัสประจำตัวของผู้เสียหายดังกล่าว เมื่อเจ้าของบัตรออกไปจากเครื่องรับฝากถอนเงินอัตโนมัติ (ตู้เอทีเอ็ม) คนร้ายก็จะแกะวัสดุที่นำไปอุดไว้ออกเพื่อนำเงินและบัตรเอทีเอ็มที่ค้างอยู่ออกมาใช้เบิกถอนเงินจากบัญชีของเจ้าของบัตรต่อไป

ซึ่งการกระทำความผิดที่เกี่ยวกับบัตรเอทีเอ็มและบัตรเดบิตนั้น ความเสียหายที่เกิดขึ้นจะน้อยกว่ากรณีการทุจริตที่เกี่ยวกับบัตรเครดิตเพราะการธุรกรรมผ่านบัตรเอทีเอ็มและบัตรเดบิตธนาคารผู้ให้บริการจะทำการหักค่าใช้จ่ายจากเงินที่คงเหลืออยู่ในบัญชีของผู้เป็นเจ้าของบัตร ดังนั้น

---

[23]เพิ่งอ้าง, น. 11.

หากธนาคารทำการหักเงินในบัญชีจนหมดแล้ว ธนาคารก็จะระงับการให้บริการผ่านบัตรดังกล่าว แต่หากเป็นกรณีของบัตรเครดิตแล้วผู้ใช้บัตรสามารถใช้บริการได้จนกว่าผู้ขอใช้บริการหรือบริษัทผู้ให้บริการจะแจ้งระงับการใช้บริการ หากตราบใดไม่มีการระงับการใช้บริการแล้วกลุ่มคนร้ายก็สามารถนำไปใช้ก่ออาชญากรรมได้ตลอดไปและค่าเสียหายก็จะมีจำนวนเพิ่มขึ้นเรื่อยๆ

2.3.3 การทำซ้ำซึ่งรหัสข้อมูลและข้อมูลในบัตรอิเล็กทรอนิกส์

2.3.3.1 การดูและจดจำ

เนื่องจากรหัสข้อมูลมีลักษณะพิเศษที่สามารถจดจำง่ายโดยใช้ตัวเลข ตัวอักษร หรือตัวเลขควบคู่กับตัวอักษร ที่มีจำนวนไม่กี่หลักและไม่ซับซ้อนมาใช้ในการกำหนดเป็นรหัสข้อมูล ดังนั้น ด้วยคุณสมบัติพิเศษของรหัสข้อมูลนี้เองเป็นช่องทางให้กลุ่มคนร้ายสามารถที่จะแอบดูและจดจำรหัสข้อมูลดังกล่าวไปใช้เพื่อเป็นเครื่องมือก่ออาชญากรรมในรูปแบบต่างๆที่เกี่ยวข้องต่อไปได้ เช่น คดีระหว่าง Lund v. Common Wealth โดย นาย Lund เข้าไปใช้คอมพิวเตอร์โดยใช้รหัสผ่านซึ่งกำหนดขึ้นโดยเพื่อนของเขา เขาถูกกล่าวหาว่าขโมยรหัสผ่าน บัตรคอมพิวเตอร์ และเครื่องพิมพ์ตลอดจนเวลาการใช้คอมพิวเตอร์ของโรงเรียนโดยปราศจากการได้รับอนุญาตโดยถูกต้อง ซึ่งศาลอุทธรณ์ได้พิพากษายกฟ้องเนื่องจากการใช้คอมพิวเตอร์ไม่เป็นการขโมยภายใต้กฎหมายของรัฐเวอร์จิเนีย (Virginia Law) นอกจากนั้นยังไม่มีกฎหมายบัญญัติว่าการได้รับแรงงานและการบริการโดยทุจริตจะเป็นความผิดอาญา ซึ่งต่อมารัฐเวอร์จิเนียก็บัญญัติกฎหมายว่าด้วยคอมพิวเตอร์โดยบัญญัติให้การกระทำทำนองเดียวกับนาย Lund เป็นความผิดและเพิ่มเป็นฐานความผิดตามกฎหมายว่าด้วยความผิดเกี่ยวกับลักทรัพย์ด้วย[24]

2.3.3.2 การดักและจับข้อมูลบนระบบเครือข่าย

เนื่องจากการทำธุรกรรมต่างๆโดยใช้รหัสข้อมูลหรือบัตรอิเล็กทรอนิกส์นั้น ส่วนใหญ่เป็นการทำธุรกรรมโดยผ่านระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นระบบการติดต่อสื่อสารที่เปิดให้บุคคลทั่วไปสามารถที่จะเข้าไปติดต่อสื่อสารได้ จึงเป็นช่องทางให้กลุ่มคนร้ายต่างๆสามารถใช้ความรู้ทางด้านเทคโนโลยีในการดักจับและทำซ้ำซึ่งรหัสข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ดังกล่าว ซึ่งการกระทำในลักษณะดังกล่าวอาจจะแบ่งออกเป็น 2 ลักษณะ คือ

---

[24]วีระพงษ์ บุญโญภาส, *อ้างแล้ว เชิงอรรถที่* 1, น. 106.

1. การเข้าถึงระบบคอมพิวเตอร์โดยตรงแล้วจึงดักจับข้อมูลที่เกิดขึ้นจากการใช้รหัสข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์นั้น เช่น

1) การใช้โปรแกรม Spy ware ซึ่งเป็นซอฟต์แวร์ชนิดหนึ่งที่ถูกออกแบบมาเพื่อทำหน้าที่คอยตรวจสอบพฤติกรรมการใช้งานของเจ้าของเครื่องคอมพิวเตอร์ว่าเจ้าของเครื่องหรือผู้ใช้เครื่องคอมพิวเตอร์นั้นได้ทำสิ่งใดกับเครื่องบ้าง ซึ่งหากผู้ใช้ได้ป้อนรหัสข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์แล้ว โปรแกรม Spy ware ก็จะทำการทำสำเนาข้อมูลที่เกิดขึ้นจากการใช้งานนั้นส่งไปยังเครื่องคอมพิวเตอร์ของกลุ่มคนร้ายผู้เป็นเจ้าของโปรแกรม Spy ware นั้น ทำให้สามารถรู้ได้ว่าข้อมูลหรือรหัสข้อมูลต่างๆที่ได้กระทำผ่านเครื่องคอมพิวเตอร์นั้นมีอะไรบ้าง[25]

2) การใช้โปรแกรม Trojan horse เป็นโปรแกรมที่กำหนดให้ทำงานโดยแฝงอยู่กับโปรแกรมทั่วไปเพื่อจุดประสงค์ใดจุดประสงค์หนึ่ง เช่น ขโมยข้อมูล เป็นต้น[26]

3) การใช้โปรแกรม Sniffer หรือเรียกว่าโปรแกรม Protocol Analyzer คือ โปรแกรมที่ทำหน้าที่ในการตรวจจับเฟรมหรือแพ็คเก็ตข้อมูล ทำให้กลุ่มคนร้ายสามารถจับเฟรมหรือแพ็คเก็ตข้อมูลที่มีรหัสผ่านอยู่ และทำให้สามารถทราบรหัสผ่านของผู้เสียหายที่ส่งหรือโอนข้อมูลผ่านระบบเครือข่ายได้[27]

4) การ Trap doors หรือประตูกล เป็นการทุจริตในขั้นตอนของการประมวลผลข้อมูล (processing) ของเครื่องคอมพิวเตอร์ โดยการเขียนโปรแกรมที่เลียนแบบคล้ายหน้าจอปกติของคอมพิวเตอร์ เพื่อลวงให้ผู้มาใช้คอมพิวเตอร์กรอกรหัสประจำตัว (ID Number) หรือรหัสผ่าน (Password) โดยโปรแกรมนี้จะเก็บข้อมูลที่ต้องการไว้ในไฟล์ลับ เพื่อนำกลับมาค้นหารหัสผ่านของผู้อื่นในภายหลัง [28]

---

[25]ถอดความมาจาก http://www.microsoft.com/thailand/security/spyware.asp

[26]สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, แนวทางการจัดทำกฎหมายอาญากรรมคอมพิวเตอร์, (ธันวาคม 2546), น. 18.

[27]ธวัชชัย ชมศิริ, Hack Step by Step, (กรุงเทพมหานคร: บริษัท ซีเอ็ด ยูเคชั่น จำกัด (มหาชน), 2546), น. 69-77.

[28]วัลลิกา อุ่นศรี, "ปัญหาการรวบรวมและพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีอาญา," (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2544), น. 41.

5) การ Scavenging คือ วิธีการค้นหาข้อมูลที่ทิ้งไว้ในระบบคอมพิวเตอร์หรือบริเวณใกล้เคียงหลังจากเสร็จงานแล้ว วิธีที่ง่ายที่สุด คือ ค้นหาตามถังขยะ (Recycle bin) ของเครื่องคอมพิวเตอร์ซึ่งอาจทำให้ได้ข้อมูลที่ทิ้งเอาไว้ เช่น รหัสผ่าน เป็นต้น[29]

6) การเข้าสู่ระบบประมวลผลโดยมิได้รับอนุญาตเพื่อจารกรรมข้อมูล (Hacking หรือ Cracking) โดยอาจเข้าไปเพื่อนำข้อมูลต่างๆที่บันทึกอยู่ในคอมพิวเตอร์ออกไปใช้ประโยชน์ เช่น รหัสข้อมูล หรือข้อมูลส่วนตัวต่างๆ เป็นต้น

2. การดักจับข้อมูลโดยผู้กระทำผิดมิได้เข้าถึงระบบคอมพิวเตอร์

1) การใช้เครื่องมือดักข้อมูล (Electronic eavesdropping devices) หรือเรียกว่าวิธี Data Leakage โดยกลุ่มคนร้ายวางเครื่องดักข้อมูลไว้ในระยะที่กำหนดเพื่อให้สามารถดักข้อมูลได้ด้วยวิธีการตรวจการแผ่รังสีของคลื่นแม่เหล็กไฟฟ้าในขณะที่เครื่องคอมพิวเตอร์กำลังทำงานเพื่อรับข้อมูล[30]

2) Wiretapping คือ การอาศัยขั้นตอนการส่งถ่ายข้อมูล Data communication ในระหว่างการทำงานของเครื่องคอมพิวเตอร์ ซึ่งอาจจะนำสายสัญญาณพาดผ่านสายส่งข้อมูลในระบบอินเตอร์เน็ตเพื่อขโมยข้อมูลโดยลักลอบดักฟังสัญญาณสื่อสารทำให้สามารถเข้าถึงข้อมูลผ่านเครือข่ายการสื่อสารนั้นได้

2.3.3.3 <u>การทำซ้ำข้อมูลที่บรรจุอยู่ในบัตรอิเล็กทรอนิกส์</u>

กรณีที่กลุ่มคนร้ายใช้เครื่องมือที่เรียกว่าเครื่องบันทึกข้อมูลในแถบแม่เหล็ก (Skimmer) ทำการคัดลอกและสำเนาข้อมูลบนบัตรที่แท้จริง โดยอาจจะต่อเครื่อง Skimmer เข้ากับเครื่องรับบัตร E.D.C. ของร้านค้าที่เป็นพรรคพวกของตน เมื่อร้านค้าผู้ให้บริการรับชำระราคาค่าสินค้าหรือบริการผ่านบัตรเครดิตของลูกค้าเมื่อใด เครื่องนี้จะทำการบันทึกรหัสแม่เหล็กหรือข้อมูลอิเล็กทรอนิกส์ที่อยู่ด้านหลังบัตรเครดิตทันที[31] หรืออาศัยโอกาสที่ตนเองได้ครอบครองหรือยึดถือบัตรดังกล่าวเพียงชั่วคราวโดยที่เจ้าของบัตรยินยอมมอบให้ เช่น ผู้ที่เจ้าของบัตรมอบให้นำบัตรดังกล่าวไปใช้สอยได้ชั่วคราว หรือกรณีได้มาโดยวิธีการใดๆที่เจ้าของมิได้อนุญาต เช่น การขโมยการเก็บบัตรอิเล็กทรอนิกส์ที่เจ้าของลืมทิ้งเอาไว้ หรือทำตกหล่น เป็นต้น ทำการคัดลอกข้อมูลที่อยู่ใน

---

[29]ทวีศักดิ์ กออนันตกูล, "อาชญากรรมในยุคโลกาภิวัฒน์," <u>บทบัณฑิตย์</u>, เล่มที่ 55 ตอน 1 (มี.ค. 2542), น. 30.

[30]*เพิ่งอ้าง*, น. 29.

[31]วีระพงษ์ บุญโญภาส, *อ้างแล้ว เชิงอรรถที่* 1, น. 302.

บัตรนั้นและเก็บข้อมูลดังกล่าวไว้เพื่อนำไปถ่ายลงหรือทำสำเนาลงในแถบแม่เหล็กหรือแผงวงจรอิเล็กทรอนิกส์ในบัตรอิเล็กทรอนิกส์ปลอมที่จัดทำขึ้นใหม่ เพื่อให้สามารถนำบัตรอิเล็กทรอนิกส์ที่ทำปลอมขึ้นนำไปใช้ได้เหมือนกับบัตรอิเล็กทรอนิกส์ที่แท้จริงในการทำอาชญากรรมที่เกี่ยวข้องต่อไป ซึ่งแต่เดิมการกระทำความผิดในลักษณะการใช้เครื่องบันทึกข้อมูลในแถบแม่เหล็ก (Skimmer) ดังกล่าวส่วนใหญ่จะเป็นการกระทำผิดต่อบัตรเครดิต แต่ในปัจจุบันเริ่มมีการนำมาใช้กับการกระทำความผิดต่อบัตรเอทีเอ็มมากยิ่งขึ้น โดยกลุ่มคนร้ายจะนำเครื่องบันทึกข้อมูลในแถบแม่เหล็กมาติดไว้ที่ช่องเสียบบัตรที่เครื่องรับฝากถอนเงินอัตโนมัติและใช้กล้องขนาดเล็กซ่อนไว้เพื่อเป็นบันทึกภาพผู้เสียหายในขณะที่กดรหัส หรือกลุ่มคนร้ายอาจจะแกล้งขอดูบัตรเอทีเอ็มจากผู้เสียหายและทำการแอบรูดกับเครื่องบันทึกข้อมูลในแถบแม่เหล็กที่ซ่อนไว้ในกระเป๋ากางเกง เป็นต้น[32]

2.3.4 <u>การโทรศัพท์หลอกลวงเพื่อให้ทราบชื่อผู้ใช้และรหัสผ่าน</u>

กรณีที่กลุ่มคนร้ายโทรศัพท์ไปหาผู้เป็นเจ้าของหรือผู้มีสิทธิเพื่อหลอกลวงให้บอกรหัสผ่าน จากนั้นกลุ่มคนร้ายจะนำชื่อผู้ใช้และรหัสผ่านไปใช้เข้าสู่ระบบฐานข้อมูลต่างๆ ซึ่งมีคดีตัวอย่าง เช่น คดี Digital Equipment Case ที่เครื่องคอมพิวเตอร์ของบริษัท U.S. Leasing มีอาการแปลกๆทำงานช้าลง ในช่วงบ่ายของวันเดียวกันได้มีคนร้ายโทรศัพท์มาแอบอ้างว่าเป็นผู้ดูแลระบบซอฟต์แวร์ของบริษัท Digital Equipment Corporation โดยหลอกว่าสาเหตุที่ทำให้เครื่องคอมพิวเตอร์ทำงานช้าเกิดขึ้นกับระบบเครือข่ายทั้งหมดของบริษัท Digital Equipment Corporation ซึ่งเขาจะแก้ไขให้แต่ต้องเข้ามาในระบบ (Access) เสียก่อน จึงขอหมายเลขบัญชีผู้ใช้ (Account Number) และรหัสผ่านของพนักงานผู้รับผิดชอบดูแลระบบของบริษัท U.S. Leasing โดยจะใช้เครื่องคอมพิวเตอร์เชื่อมต่อเข้าสู่ระบบคอมพิวเตอร์ของบริษัท U.S. Leasing เข้ามาแก้ไขปัญหาให้และรับประกันว่าทุกอย่างจะคืนสู่สภาพปกติ แต่ปรากฏว่าระบบคอมพิวเตอร์ยังทำงานช้าอยู่เหมือนเดิม ผู้อำนวยการฝ่ายระบบของบริษัท U.S. Leasing จึงติดต่อไปยังบริษัท Digital Equipment Corporation จึงพบว่าถูกกลุ่มคนร้ายหลอกลวงเพื่อให้ได้ไปซึ่งหมายเลขบัญชีผู้ใช้และรหัสผ่าน และกลุ่มคนร้ายได้ทำให้เครื่องพิมพ์ (printer) ที่เชื่อมต่อกับเครื่องคอมพิวเตอร์พิมพ์กระดาษออกมาเต็มห้องพร้อมข้อความหยาบคาย นอกจากนั้นยังลบข้อมูลของบริษัทในระบบฐานข้อมูลจนหมด[33]

---

[32]กองบรรณาธิการ, *อ้างแล้ว เชิงอรรถที่* 14, น. 218.

[33]*ทวีศักดิ์ กออนันตกูล, อ้างแล้ว เชิงอรรถที่* 29, น. 34-35.

แต่เนื่องจากในปัจจุบันได้มีการหลอกลวงโดยการใช้วิธีอื่นนอกเหนือจากการใช้โทรศัพท์เพื่อหลอกลวงให้ทราบชื่อผู้ใช้และรหัสผ่าน โดยใช้วิธีการหลอกลวงผ่านระบบอินเตอร์เน็ต ซึ่งเรียกวิธีดังกล่าวว่า "ฟิชชิ่ง (Phishing)" คือ การที่แฮกเกอร์ส่งอีเมล์ปลอมหรือปลอมแปลงข้อความถึงเหยื่อโดยอ้างว่ามาจากองค์กรต่างๆที่เหยื่อติดต่อด้วย เช่น บริษัทผู้ให้บริการอินเตอร์เน็ตหรือธนาคารที่เหยื่อมีบัญชีอยู่ด้วยเพื่อหลอกให้เปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลหมายเลขบัตรเครดิต ชื่อผู้ใช้ รหัสผ่าน รหัสประจำตัว ผ่านเวปไซต์ที่ทำหลอกขึ้น (Spoofed Website) แต่มี URL เหมือนกับธนาคารหรือองค์กรนั้น เมื่อผู้รับจดหมายหลงเชื่อและเข้าสู่เวปไซต์ปลอมเหล่านี้ก็อาจถูกหลอกลวงให้กรอกข้อมูลส่วนตัวที่จะถูกส่งไปยังผู้ผลิตเวปไซต์แล้วนำข้อมูลไปใช้ประโยชน์ เช่น ซื้อสินค้า สมัครบัตรเครดิต หรือแม้แต่ทำสิ่งที่ผิดกฎหมายอื่นๆในนามของเจ้าของข้อมูลนั้น[34]

2.3.5 <u>การปลอมแปลงบัตรอิเล็กทรอนิกส์</u>

2.3.5.1 <u>บัตรปลอม</u> (Counterfeit Card) คือ การที่คนร้ายทำการปลอมบัตรอิเล็กทรอนิกส์ขึ้นทั้งฉบับให้เหมือนกับบัตรอิเล็กทรอนิกส์ที่แท้จริงทุกประการ โดยใช้บัตรพลาสติกที่มีขนาดเท่ากับบัตรที่แท้จริงแล้วนำข้อมูลที่อยู่ในแถบแม่เหล็กด้านหลังบัตรที่แท้จริงที่เตรียมไว้ทำการปลอมแปลงบัตรโดยใช้เครื่องพิมพ์ (Embossing Machine) และบันทึกข้อมูลลงในบัตรที่ปลอมแปลงขึ้น หรือกรณีที่พนักงานของบริษัทคอมพิวเตอร์แห่งหนึ่งซึ่งได้รับการว่าจ้างจากธนาคารแห่งหนึ่งให้ดูแลระบบเครื่องรับฝากถอนเงินอัตโนมัติ แอบเขียนโปรแกรมซ่อนไว้ในระบบคอมพิวเตอร์เพื่อจัดเก็บข้อมูลบัตรเอทีเอ็มพร้อมรหัสของลูกค้าของธนาคาร หลังจากนั้นได้ทำบัตรเอทีเอ็มปลอมที่บันทึกข้อมูลจากบัตรเอทีเอ็มของลูกค้าธนาคารนำไปใช้พร้อมกับรหัสเพื่อเบิกเงินจากบัญชีของลูกค้า เป็นต้น

2.3.5.2 <u>การแปลงข้อมูลจากบัตรจริง</u> (Altered Card) คือ การนำบัตรอิเล็กทรอนิกส์ที่หมดอายุแล้วนำมาเปลี่ยนแปลงข้อมูลเดิมออกด้วยวิธีการรีดด้วยความร้อนให้ข้อมูลที่พิมพ์อยู่บนบัตรเดิมที่เป็นตัวนูนเรียบลง จากนั้นจึงนำข้อมูลของบัตรอิเล็กทรอนิกส์ที่ยังสามารถใช้บริการได้ทำการปั๊มข้อมูลลงบนบัตรปลอม ซึ่งเรียกว่า วิธีการ Re–Embossed หรือมีการบันทึกรหัสแม่เหล็กของผู้อื่นลงในแถบแม่เหล็ก ซึ่งเรียกว่า Re–Embossed Card จากนั้นจึงทำการขูดแถบลายเซ็น

---

[34]กองบรรณาธิการ, "แบงก์เตือน E-mail มหาภัยหลอกชโมยเงิน," <u>วารสารการเงินการธนาคาร</u>, ฉบับที่ 279 (กรกฎาคม 2548), น. 170-178.

เก่าออกแล้วใช้สติ๊กเกอร์ที่มีลักษณะเลียนแบบแถบลายเซ็นเก่ามาปิดทับลงไปเพื่อจะได้เซ็นชื่อใหม่ให้สอดคล้องกับชื่อด้านหน้าบัตรที่แก้ไขใหม่ แล้วนำไปใช้ซื้อสินค้าและบริการจากร้านค้าหรือสถานประกอบการอื่นต่อไป[35]

2.3.5.3 บัตรพลาสติกขาว (White Plastic Card) คือ การนำเอาแผ่นพลาสติกสีขาวที่มีความหนาและขนาดเท่ากับบัตรเครดิตมาทำการปั๊มข้อมูลอิเล็กทรอนิกส์ของบัตรเครดิตที่แท้จริง เช่น หมายเลขบัตรเครดิต ระยะเวลาที่ใช้บัตรได้ และชื่อของผู้ถือบัตร ลงในบัตรพลาสติกขาว นำไปใช้กับร้านค้าต่างๆซึ่งเป็นของพวกกลุ่มคนร้าย ซึ่งบัตรพลาสติกขาวจะแตกต่างจากบัตรที่ทำขึ้นโดยการปลอม หรือบัตรที่แปลงข้อมูลบนบัตร เพราะจะไม่มีลวดลายของบัตรเหมือนกับบัตรที่แท้จริง

2.3.6 การใช้รหัสข้อมูลและข้อมูลในบัตรอิเล็กทรอนิกส์ของผู้มีสิทธิโดยทุจริต

การกระทำผิดในลักษณะนี้จะเป็นการลงมือกระทำผิดโดยผู้ที่เป็นเจ้าของบัตรหรือข้อมูลในบัตรอิเล็กทรอนิกส์นั้นเอง เพื่อที่จะหลีกเลี่ยงไม่ต้องชำระค่าบริการให้แก่บริษัทผู้ให้บริการ เช่น การลบข้อมูลการใช้จ่ายบัตรของผู้ถือบัตรในเครื่องประมวลผลของธนาคารหรือบริษัทผู้ให้บริการ ซึ่งจะเป็นการทุจริตที่ร่วมมือกันระหว่างผู้ถือบัตรและเจ้าหน้าที่ของธนาคารหรือบริษัทผู้ออกบัตร โดยเมื่อผู้ถือบัตรนำบัตรไปใช้ซื้อสินค้าหรือบริการจากร้านค้าต่างๆจนครบวงเงินแล้วก็จะให้เจ้าหน้าที่ของธนาคารหรือบริษัทผู้ออกบัตรทำการลบข้อมูลการใช้บัตรเครดิตที่บันทึกอยู่ในระบบคอมพิวเตอร์ของธนาคารหรือบริษัทผู้ออกบัตร ทำให้ธนาคารหรือบริษัทผู้ออกบัตรไม่อาจจะเรียกเก็บเงินจากผู้ถือบัตรได้ เพราะไม่ปรากฏรายการใช้บัตรอีกต่อไป[36]

2.3.7 การใช้รหัสข้อมูลและข้อมูลในบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยทุจริต

2.3.7.1. การลักลอบใช้โดยทุจริต คือ การที่กลุ่มคนร้ายนำรหัสข้อมูล ข้อมูลที่อยู่ในบัตรอิเล็กทรอนิกส์ หรือบัตรอิเล็กทรอนิกส์ของผู้อื่นที่ได้จากการกระทำความผิดในรูปแบบต่างๆไปก่ออาชญากรรม เช่น

---

[35]สุรเชษฐ์ ชีววินิจ, *อ้างแล้ว เชิงอรรถที่* 22, น. 12.

[36]*เพิ่งอ้าง*, น. 16.

1) การใช้รหัสข้อมูลเพื่อถอนเงินจากธนาคาร คือ หลังจากที่กลุ่มคนร้ายได้ทำการหลอกลวงเพื่อให้ได้มาซึ่งบัตรเอทีเอ็มของผู้อื่นและจดจำรหัสบัตรดังกล่าวได้แล้วก็จะนำบัตรเอทีเอ็มพร้อมรหัสบัตรไปดำเนินการเบิกถอนเงินจากเครื่องรับฝากถอนเงินอัตโนมัติ โดยวงเงินที่สามารถเบิกถอนได้จะขึ้นอยู่กับจำนวนเงินฝากของผู้เป็นเจ้าของบัญชีว่ามีอยู่จำนวนมากน้อยเพียงใด ซึ่งเป็นการก่อให้เกิดความเสียหายให้กับทั้งผู้เป็นเจ้าของบัตรที่แท้จริงและธนาคารผู้รับฝากเงินด้วย

2) การใช้รหัสข้อมูลเพื่อเติมเงินค่าใช้บริการโทรศัพท์ คือ โดยปกติทั่วไปในการใช้บริการโทรศัพท์เคลื่อนที่ในระบบเติมเงิน (ระบบ pre-paid) ในปัจจุบัน ก่อนที่ผู้ใช้บริการจะสามารถใช้บริการโทรศัพท์ได้จะต้องมีการชำระค่าบริการล่วงหน้าหรือเรียกว่าการเติมเงินเข้าสู่ระบบของบริษัทผู้ให้บริการเสียก่อน ซึ่งวิธีที่ใช้เติมเงินอย่างแพร่หลาย ก็คือ การเติมเงินโดยใช้บัตรเติมเงินที่จะมีการกำหนดจำนวนยอดเงินที่ต้องการจะเติมไว้ล่วงหน้าจำหน่ายให้แก่ผู้ใช้บริการ เช่น 50 บาท 100 บาท 150 บาท หรือ 300 บาท เป็นต้น โดยที่บริษัทผู้ให้บริการจะกำหนดชุดตัวเลขขึ้นชุดหนึ่งระบุไว้บนบัตรเติมเงินเพื่อใช้เป็นเครื่องหมายแทนมูลค่าของบัตรเติมเงินนั้น ซึ่งตัวเลขชุดดังกล่าวจะสามารถใช้ได้ครั้งเดียว ดังนั้น หากกลุ่มคนร้ายทำการแอบดูและจดจำชุดตัวเลขดังกล่าวและนำไปใช้เติมเงินเข้าสู่ระบบก่อนที่ผู้ที่ซื้อบัตรเติมเงินจะได้ทำการเติมเงินเข้าสู่หมายเลขโทรศัพท์ของตนแล้ว ย่อมทำให้เกิดความเสียหายแก่ผู้ที่ได้ซื้อบัตรดังกล่าวเพราะไม่สามารถใช้ประโยชน์จากบัตรเติมเงินดังกล่าวได้อีกต่อไป

3) การใช้รหัสข้อมูลเพื่อตรวจดูกล่องจดหมายอิเล็กทรอนิกส์ (Mail Box) คือ เมื่อมีการนิยมนำการส่งจดหมายในรูปของสื่ออิเล็กทรอนิกส์ หรือที่เรียกว่า electronic mail มาใช้กันอย่างแพร่หลายมากขึ้น ไม่ว่าจะเป็นในการติดต่อในการเสนอซื้อหรือเสนอขาย หรือการติดต่อระหว่างคู่สัญญาในการค้าพาณิชย์อิเล็กทรอนิกส์ หรือนำมาใช้ในการติดต่อยื่นซองประกวดราคาในระบบการประมูลทางอิเล็กทรอนิกส์ (e-auction) หรือแม้กระทั่งในการส่งจดหมายถึงกันระหว่างบุคคล จึงทำให้ตู้จดหมายอิเล็กทรอนิกส์ (mail box) ซึ่งเปรียบเสมือนตู้เก็บจดหมายมีความสำคัญตามไปด้วย ดังนั้น หากกลุ่มคนร้ายทราบถึง E-mail address ผู้ใช้บริการ รหัสผ่าน และนำรหัสข้อมูลดังกล่าวไปใช้เข้าสู่ตู้จดหมายอิเล็กทรอนิกส์ แล้วย่อมจะทราบถึงข้อมูลที่ได้มีการโต้ตอบระหว่างผู้เป็นเจ้าของตู้จดหมายอิเล็กทรอนิกส์กับบุคคลภายนอก เช่น ข้อมูลทางการค้า ข้อมูลส่วนตัว เป็นต้น ทำให้สามารถนำข้อมูลดังกล่าวไปใช้ในการประกอบอาชญากรรมในรูปแบบอื่นๆได้ต่อไป เช่น หากจดหมายอิเล็กทรอนิกส์นั้นเป็นจดหมายที่บริษัทผู้ให้บริการระบบฐานข้อมูลออนไลน์ต่างๆที่ต้องเสียค่าบริการส่งชื่อผู้ใช้และรหัสผ่านในการเข้าใช้บริการให้แก่ผู้เป็นเจ้าของตู้จดหมายอิเล็กทรอนิกส์แล้ว

เมื่อกลุ่มคนร้ายเข้าสู่ระบบได้ย่อมจะใช้บริการดังกล่าว ทำให้ผู้ที่มีสิทธิใช้ที่แท้จริงได้รับความเสียหายเพราะจะต้องเสียค่าบริการให้แก่บริษัทผู้ให้บริการทั้งๆที่ตนไม่ได้ใช้บริการแต่อย่างใด อีกทั้ง การเข้าสู่ตู้จดหมายอิเล็กทรอนิกส์ยังเป็นการละเมิดสิทธิส่วนตัวของผู้เป็นเจ้าของตู้จดหมายอิเล็กทรอนิกส์อีกด้วย เป็นต้น

4) การใช้รหัสข้อมูลเพื่อลักลอบใช้บริการ คือ เมื่อกลุ่มคนร้ายสามารถทราบรหัสข้อมูลที่ใช้ในการเข้าสู่ระบบเครือข่ายและสามารถเข้าสู่ระบบดังกล่าวของผู้เสียหายได้แล้ว กลุ่มคนร้ายก็จะกระทำการต่างๆเพื่อแสวงหาประโยชน์จากระบบเครือข่ายของบริษัทผู้ให้บริการ เช่น การใช้บริการโทรศัพท์ผ่านเครือข่ายของบริษัทผู้ให้บริการ ซึ่งมีคดีตัวอย่างที่เกิดขึ้นในต่างประเทศ คือ คดี United State v. Patrick W. Grego ในช่วงปี 1997-1999 กลุ่มนักเจาะระบบที่ใช้ชื่อว่า totle – Kaos และ global Hell ได้เจาะเข้าสู่ระบบเพื่อขโมยอุปกรณ์การเข้าถึงโดยไม่ได้รับอนุญาต (unauthorized access device) ได้แก่ หมายเลขโทรศัพท์ รหัสประจำตัว (PIN) และหมายเลขบัตรเครดิต รวมทั้งนำอุปกรณ์ดังกล่าวไปติดตั้งให้บริการประชุมโทรภาพทางไกล (teleconference) ในหมู่สมาชิกโดยไม่ได้รับอนุญาต และแอบฟังการประชุมของบุคคลอื่น ซึ่งศาลตัดสินให้ลงโทษจำคุก 26 เดือน และชดใช้ค่าเสียหายจำนวน 154,529.86 เหรียญสหรัฐ[37]

5) การใช้รหัสข้อมูลเพื่อเข้าใช้บริการชั่วโมงอินเตอร์เน็ต คือ การที่กลุ่มคนร้ายนำชื่อผู้ใช้และรหัสผ่านที่ได้จากการกระทำความผิดในรูปแบบต่างๆ เช่น การแอบดูในขณะที่ผู้เป็นเจ้าของหรือผู้มีสิทธิใช้บริการกรอกรหัสข้อมูลดังกล่าวเพื่อเชื่อมต่อระบบอินเตอร์เน็ต การค้นหาจากถังขยะ (Recycle Bin) หรือการเจาะเข้าสู่ระบบเพื่อขโมยรหัสข้อมูลดังกล่าวไปกระทำความผิดเพื่อหาประโยชน์ให้แก่ตนเองโดยมิชอบด้วยกฎหมาย ซึ่งมีคดีตัวอย่าง เช่น คดี United State v. Andrew Miffleton จำเลยเป็นผู้มีความรู้เชี่ยวชาญด้านคอมพิวเตอร์ได้ทำการเจาะ (hack) เข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตและมีรหัสผ่านคอมพิวเตอร์ของบริษัทอินเตอร์เน็ตในระดับที่สามารถเข้าควบคุมระบบคอมพิวเตอร์ได้ทั้งหมด ซึ่งจำเลยนำไปใช้เข้าสู่ (access) ระบบคอมพิวเตอร์ทั่วประเทศโดยไม่ได้รับอนุญาต นอกจากนั้นยังเป็นเจ้าของ access device โดยไม่ได้รับอนุญาตอันได้แก่ รหัสผ่านของผู้ให้บริการอินเตอร์เน็ตที่มีไว้ให้บริการบุคคลทั่วไป หมายเลขประจำเครื่อง หรือหมายเลขสำหรับใช้บริการโทรศัพท์ในระบบ cellular หมายเลขบัตรโทรศัพท์เพื่อ

---

[37]สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ, (ธันวาคม 2546), น. 63.

ใช้ในการโทรศัพท์ทางไกล และหมายเลขบัตรเครดิต ซึ่งศาลตัดสินว่ามีความผิดตาม title 18 *United States Code* section 1029(a)(3)[38]

หรือ คดี United State v. Raymond Torricelli จำเลยใช้โปรแกรมที่เรียกว่า"rootkit" ซึ่งเป็นโปรแกรมที่หากนำไปใช้รัน (run) บนเครื่องคอมพิวเตอร์ใดจะสามารถใช้งานได้ทุกหน้าที่ (functions) ของเครื่องนั้นโดยไม่ต้องได้รับอนุญาตก่อน ซึ่งจำเลยได้ใช้โปรแกรมนี้ในการติดตั้งโปรแกรมเพื่อดักฟัง (intercept) ชื่อผู้ใช้และรหัสผ่านจากเครื่องที่เข้ามาเชื่อมต่อเพื่อนำใช้ในการเข้าอินเตอร์เน็ต ซึ่งศาลมีคำพิพากษาให้ลงโทษปรับและจำคุก[39] เป็นต้น

6) การใช้เลขหมายบัตรเครดิตเพื่อทำธุรกรรมทางอินเตอร์เน็ต คือ การที่กลุ่มคนร้ายนำหมายเลขบัตรเครดิตที่ได้ทำการคัดลอกและจดจำมาจากบัตรเครดิตของผู้เป็นเจ้าของที่แท้จริงหรือผู้ที่มีสิทธิใช้ ไปกระทำความผิดเพื่อหาประโยชน์ให้แก่ตนเองโดยมิชอบด้วยกฎหมาย ซึ่งมีคดีตัวอย่าง เช่น คดีระหว่าง United State v. Bice-Bey โดย Bice-Bey เป็นร้านค้าที่ได้รับคำสั่งซื้อสินค้าทางโทรศัพท์ (Telephone order) หลายครั้ง ซึ่งมีการชำระราคาโดยใช้หมายเลขบัตรเครดิต จากการตรวจสอบพบว่าการสั่งซื้อสินค้าทางโทรศัพท์และชำระราคานั้นเกิดขึ้นโดยทุจริต คือ เป็นการใช้หมายเลขบัตรเครดิตของผู้อื่นโดยไม่มีอำนาจ (เอาเฉพาะหมายเลขบัตรเครดิตของผู้อื่นมาใช้) เจ้าหน้าที่ตำรวจสอบสวนกลาง (FBI) ได้ปลอมตัวเข้าไปเป็นพนักงานของร้าน Bice-Bey และสามารถสืบสวนจับกุมเจ้าของร้านได้ในข้อหาใช้หมายเลขบัตรเครดิตโดยฉ้อฉล เจ้าของร้านต่อสู้ว่าหมายเลขบัตรเครดิตไม่ใช่บัตรเครดิต ศาลสหรัฐอเมริกาตัดสินว่า หมายเลขบัตรเครดิต คือองค์ประกอบสำคัญของบัตรเครดิต การที่ Bice-Bey เอาหมายเลขบัตรเครดิตไปใช้ย่อมทราบดีว่าหมายเลขบัตรเครดิตไม่ใช่ของตน การได้หมายเลขบัตรเครดิตนั้นมาเป็นการได้มาโดยการฉ้อฉล จึงต้องรับโทษ ซึ่งแสดงให้เห็นจุดสำคัญของการทุจริตต่อบัตรเครดิตนั้นรวมทั้งการนำหมายเลขบัตรเครดิตไปใช้โดยมิชอบด้วย[40]

หรือ คดี Hacker ที่เป็นวัยรุ่นชื่อ Raphael Gray อายุ 18 ปี ได้บุกรุกเข้าไปยังเวปไซต์ที่ให้บริการ E-commerce ต่างๆจนสามารถขโมยหมายเลขบัตรเครดิตมาได้เป็นจำนวนกว่า 26,000 หมายเลข ซึ่งในจำนวนนั้นมีหมายเลขบัตรเครดิตของนายบิลล์ เกตส์ ประธานบริษัท Microsoft

---

[38]*เพิ่งอ้าง*, น. 60.

[39]*เพิ่งอ้าง*, น. 61.

[40]สุรเชษฐ์ ชีรวินิจ, โกงสะบัด โกงสะบัตร, (กรุงเทพมหานคร: บริษัท คอมฟอร์ม จำกัด, 2541), น. 218.

รวมอยู่ด้วย เจ้าหน้าที่ FBI ออกมาให้ข้อมูลเกี่ยวกับการจับกุมในครั้งนี้ว่า ได้จับกุม Raphael Gray และเพื่อนผู้สมคบคิดในการขโมยบัตรเครดิตจำนวนกว่า 26,000 หมายเลข จากเวปไซต์ E–commerce เล็กๆทั่วโลกถึง 8 แห่ง โดยที่เป็นเวปไซต์ที่อยู่ในประเทศสหรัฐอเมริกา แคนาดา ไทย ญี่ปุ่น และอังกฤษ โดยผู้กระทำความผิดอาศัยช่องโหว่ในโปรแกรมของ Microsoft เจาะเข้าไปยังฐานข้อมูลดังกล่าว โดยเริ่มกระทำความผิดครั้งแรกในเดือนมกราคม 2544 ที่เวปไซต์ซึ่งเป็นของ ISP (Internet Service Provider) รายหนึ่งในประเทศไทย นั่นคือ www.shoppingthailand.com และในคราวนั้นเขาได้หมายเลขบัตรเครดิตไปกว่า 1,000 หมายเลข และนำหมายเลขบัตรเครดิตพร้อมชื่อเจ้าของบัตรไปโพสต์ไว้บนเวปไซต์ส่วนตัวที่ www.xoom.com และต่อมาอีกไม่นานเขาและเพื่อนได้เข้าไปขโมยข้อมูลบัตรเครดิตจากเวปไซต์ E–commerce รายอื่นๆ เช่น www.promobility.net , www.itamedia.com , www.ascp.org , www.ntd.co.uk เป็นต้น โดยความเสียหายที่เกิดขึ้นในครั้งนี้คาดว่าจะมีมูลค่าสูงถึง 3 ล้านดอลลาร์สหรัฐ[41] เป็นต้น

2.3.7.2 การรูดบัตรซ้ำ (Multiple Imprint / Record of Charge Pumping) คือ การทุจริตของร้านค้าหรือพนักงานของร้านค้าที่รูดบัตรกับเครื่องรับบัตร E.D.C. หลายครั้ง เพื่อทำใบบันทึกรายการขายไว้หลายชุด แต่นำใบบันทึกรายการขายมาให้ผู้ถือบัตรเซ็นชื่อเพียงชุดเดียว ส่วนชุดที่เหลือร้านค้าหรือพนักงานที่ทุจริตจะปลอมลายมือชื่อของผู้ถือบัตรแล้วส่งไปเรียกเก็บเงินจากธนาคารหรือบริษัทผู้ออกบัตรในภายหลัง ซึ่งวิธีการนี้ถ้าผู้ถือบัตรไม่ตรวจสอบรายการใช้ให้ดีก็อาจจะจ่ายเงินให้กับธนาคารหรือบริษัทผู้ออกบัตรไป[42]

2.3.7.3 การแก้ไขจำนวนเงินในบันทึกรายการขาย (Sales Slip) คือ การที่ร้านค้าทำการแก้ไขราคาสินค้าโดยกรอกราคาสินค้าหรือบริการให้สูงกว่าความเป็นจริง ทั้งในขณะที่ทำการบันทึกรายการขายหรือกระทำภายหลังก่อนที่จะนำใบบันทึกรายการขายไปเรียกเก็บเงินจากธนาคารหรือบริษัทผู้ออกบัตร[43] เช่น ผู้ถือบัตรทำการซื้อสินค้าหรือเบิกถอนเงินสดโดยผ่าน

---

[41]กองบรรณาธิการ, " Hot News" Internet Magazine, ปีที่ 5 ฉบับที่ 3(45)(เดือนมีนาคม 2543) , น. 25-26, อ้างใน วุฒิพงศ์ เถาวัฒนะ, "พาณิชย์อิเล็กทรอนิกส์:ศึกษากรณีป้องกันการทุจริตในการใช้บัตรเครดิตบนอินเตอร์เน็ต ," (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2544), น. 37.

[42]สุรเชษฐ์ ชีรวินิจ, *อ้างแล้ว เชิงอรรถที่* 22, น. 12.

[43]*เพิ่งอ้าง*, น. 15.

บัตรเครดิตจำนวน 5,000 บาท ซึ่งในใบบันทึกรายการการขายก็จะปรากฏจำนวนเงิน 5,000 บาท ทั้งสามฉบับ และส่งสำเนา 1 ฉบับให้แก่ผู้ถือบัตรเก็บไว้ พอสิ้นวันพนักงานจะสรุปยอดเงินนำใบบันทึกรายการขายส่งธนาคารก็จะทำการเพิ่มตัวเลข 1 ลงหน้า 5,000 บาท เป็น 15,000 บาท ซึ่งจำนวนเงิน 10,000 บาท ที่เกินนี้ พนักงานผู้รับบัตรจะยักยอกไว้เป็นประโยชน์ส่วนตัว ธนาคารผู้รับบัตรจะทราบก็ต่อเมื่อลูกค้าผู้ถือบัตรปฏิเสธการจ่ายเงินกับธนาคารหรือบริษัทผู้ออกบัตร และแสดงหลักฐานว่าได้เบิกเงินเพียง 5,000 บาท เท่านั้น[44]

[44] *เพิ่งอ้าง.*