บทที่ 3

หลักกฎหมายและมาตรการป้องกันการทุจริตในการใช้บัตรเครดิตบนอินเตอร์เนทของต่างประเทศ

การทุจริตต่อบัตรเครดิตบนอินเตอร์เนท เป็นการกระทำผิดที่คอมพิวเตอร์เข้ามามีส่วนเกี่ยวข้อง โดยคนร้ายจะนำหมายเลขบัตรเครดิตของผู้อื่นไปใช้แสวงหาประโยชน์โดยมิชอบด้วยการสั่งซื้อสินค้าและบริการจากเว็บไซต์ต่างๆ ที่จัดตั้งขึ้นบนเครือข่ายอินเตอร์เนท เมื่อพิจารณาถึงการได้มาซึ่งหมายเลขบัตรเครดิตของผู้อื่นมาไว้ในครอบครองได้นั้น อาจเกิดจากการขโมยข้อมูลส่วนบุคคลของผู้อื่นไปใช้ในการยื่นขอสมัครเป็นผู้ถือบัตรเครดิต การขโมยบัตรเครดิตของผู้อื่น หรือการเก็บบัตรเครดิตของผู้อื่นได้จากการสูญหาย เป็นต้น ซึ่งกรณีดังกล่าวทำให้คนร้ายได้ครอบครองทั้งตัวบัตรและข้อมูลในบัตรนั้น อีกส่วนหนึ่งของการได้มานั้นอาจเกิดจากการขโมยข้อมูลผ่านระบบคอมพิวเตอร์และเครือข่ายอินเตอร์เนท ซึ่งการกระทำเช่นนี้จัดเป็นรูปแบบหนึ่งของอาชญากรรมคอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่ง ซึ่งไม่สามารถใช้อาวุธปราบปรามได้โดยตรง อีกทั้งยังมีส่วนเกี่ยวข้องในชีวิตประจำวันเป็นอย่างมาก ผู้กระทำผิดด้านนี้เป็นผู้มีความรู้ มีตำแหน่งหน้าที่การงาน มีประสบการณ์และความชำนาญสูง และมีผลประโยชน์เข้ามาเกี่ยวข้องจำนวนมหาศาล แต่กฎหมายบ้านเราที่จะเข้าถึงเรื่องเหล่านี้ค่อนข้างยาก แม้ว่าจะมีประมวลกฎหมายอาญาใช้นานแล้วก็ตาม แต่ก็ยังไม่มีกฎหมายที่จะจัดการกับอาชญากรรมประเภทนี้โดยเฉพาะ[1] ดังนั้น การคุ้มครองข้อมูลส่วนบุคคลของผู้อื่น การควบคุมอาชญากรรมคอมพิวเตอร์ รวมถึงการจัดระบบรักษาความปลอดภัยของข้อมูลในการทำธุรกรรมต่างๆ บนระบบคอมพิวเตอร์และเครือข่ายอินเตอร์เนท จึงมีความสำคัญอย่างยิ่งที่จะต้องพิจารณาควบคู่กันไป

---

[1] วีระพงษ์ บุญโญภาส, A specialized Seminar for Mid-and Clypper-Level Royal Thai Police Executives, Computer-Related Crime Issues and Trends , November 24-30, 1996 Pattaya Thailand. อ้างถึงใน พ.ต.ท.พงศ์ธร บุญอารีย์, กฎหมายระหว่างประเทศในส่วนที่เกี่ยวกับคดีอาญา, (กรุงเทพมหานคร : สำนักพิมพ์วิญญูชน, 2540) , หน้า 175.

ประเทศสหรัฐอเมริกานับว่าเป็นต้นกำเนิดของบัตรเครดิต ทั้งยังเป็นประเทศที่ได้รับการยอมรับจากทั่วโลกว่ามีการพัฒนาระบบเทคโนโลยีในระดับสูง แต่ในขณะเดียวกันการกระทำทุจริตต่อบัตรเครดิตบนอินเตอร์เนทรวมถึงการก่ออาชญากรรมทางคอมพิวเตอร์ในรูปแบบต่างๆ ก็เกิดขึ้นเป็นจำนวนมาก อันเป็นผลให้มีการพัฒนากฎหมายที่เกี่ยวข้องอย่างต่อเนื่องเพื่อรองรับกับปัญหาต่างๆ ที่เกิดขึ้น นอกจากนี้ประเทศในสหราชอาณาจักรโดยเฉพาะประเทศอังกฤษก็ให้ความสำคัญถึงปัญหาเหล่านี้และมีพัฒนาการด้านกฎหมายที่เกี่ยวข้องกับเทคโนโลยีเช่นกัน อันสมควรนำมาศึกษาเพื่อหาจุดเหมาะสมในการพัฒนากฎหมายของประเทศไทยต่อไป

สภาพปัญหาพาณิชย์อิเล็คทรอนิคส์ในประเทศสหรัฐอเมริกา

ท่าทีที่เป็นทางการของสหรัฐฯ ต่อการพาณิชย์อิเล็คทรอนิคส์ถูกแสดงออกในเอกสารเรื่อง "A Framework for Global Electronics Commerce" ของประธานาธิบดีคลินตัน[2] ในเอกสารดังกล่าวซึ่งสหรัฐฯจะใช้เป็นร่างข้อเสนอให้นานาประเทศยอมรับเพื่อนำไปจัดทำความตกลงกัน โดยได้กำหนดประเด็นที่นานาประเทศจะต้องมีการหารือกัน เพื่อส่งเสริมให้เกิดพาณิชย์อิเล็คทรอนิคส์ผ่านอินเตอร์เนทโดยไม่ต้องมีการกำกับดูแลโดยรัฐ 9 ประเด็น สองประเด็นแรกเกี่ยวข้องกับการเงิน สี่ประเด็นต่อมาเกี่ยวข้องกับกฎหมาย และสามประเด็นสุดท้ายเกี่ยวข้องกับการเข้าสู่ตลาด

1. ภาษีและการศุลกากร (Custom and Taxation) อินเตอร์เนทควรได้รับการประกาศให้เป็นเขตปลอดภาษีศุลกากร (Tariff-free) ในการจำหน่ายสินค้าและบริการที่มีการจัดส่งผ่านอินเตอร์เนท เนื่องจากทุกประเทศที่เกี่ยวข้องจะได้ประโยชน์ ประเทศต่างๆ จึงไม่ควรจัดเก็บภาษีใหม่ใดๆ เพิ่มเติมจากการพาณิชย์อิเล็คทรอนิคส์ผ่านอินเตอร์เนท นอกจากนี้ ภาษีที่จะจัดเก็บจากการพาณิชย์อิเล็คทรอนิคส์ จะต้องสอดคล้องกับระบบภาษีระหว่างประเทศที่มีอยู่ และต้องง่ายต่อการบริหาร

2. ระบบการชำระเงินอิเล็คทรอนิคส์ (Electronic Payment System) เป็นการ

---

[2] ข้อมูลดังกล่าวแปลมาจาก A Framework for Global Electronics Commerce ใน Http://iitf.doc.gov/electronic_commerce.htm (20 May 2001).

ยากที่จะสามารถออกแบบระบบการชำระเงินที่เหมาะสม และทันกับการเปลี่ยนแปลง ดังนั้น นโยบายต่อประเด็นนี้ควรมีความคล่องตัวและยืดหยุ่น ในอนาคตอันใกล้นี้ เราควรเฝ้าดูการทดลองการชำระเงินอิเล็คทรอนิคส์เป็นกรณีไป

3. กฎระเบียบทางการค้า (Commercial Code) สหรัฐฯ สนับสนุนให้เกิดกฎระเบียบระหว่างประเทศที่เป็นอันหนึ่งอันเดียวกัน (Uniform) ในการสนับสนุนการพาณิชย์อิเล็คทรอนิคส์ กฎระเบียบระหว่างประเทศดังกล่าวควรจะสนับสนุนให้มีการรับรองการทำสัญญาทางอิเล็คทรอนิคส์ ลายมือชื่ออิเล็คทรอนิคส์ และขั้นตอนการรับรองอื่นๆ ส่งเสริมกลไกการระงับข้อขัดแย้ง กำหนดขอบเขตของความรับผิดชอบของฝ่ายต่างๆ และเร่งรัดการจดทะเบียนทางอิเล็คทรอนิคส์

4. การคุ้มครองทรัพย์สินทางปัญญา (Intellectual property protection) การพาณิชย์อิเล็คทรอนิคส์มักจะเกี่ยวข้องกับการขายหรืออนุญาตให้ใช้ทรัพย์สินทางปัญญา เพื่อส่งเสริมการพาณิชย์อิเล็คทรอนิคส์ ผู้ขายสินค้าและบริการจะต้องได้รับหลักประกันในการคุ้มครองสิทธิในทรัพย์สินทางปัญญาของตน ในขณะที่ผู้ซื้อจะต้องได้หลักประกันว่าสินค้าที่ตนซื้อมาเป็นสินค้าที่ถูกต้องที่ไม่ได้ละเมิดทรัพย์สินทางปัญญาของผู้อื่น สหรัฐฯ ยังให้ความสำคัญต่อการคุ้มครองทรัพย์สินทางปัญญา ที่เกี่ยวข้องกับเทคโนโลยีของอินเตอร์เนทและประเด็นทางทรัพย์สินทางปัญญาใหม่ๆ เช่น การคุ้มครองชื่อโดเมน (Domain name) โดยกำลังพยายามศึกษาหาแนวทางในการใช้กลไกตลาดในการคุ้มครองทรัพย์สินทางปัญญาเหล่านี้

5. การคุ้มครองข้อมูลส่วนตัวของผู้บริโภค (Privacy) สหรัฐฯ เป็นประเทศที่ให้ความสำคัญต่อการคุ้มครองข้อมูลส่วนตัวของประชาชนเป็นอย่างยิ่ง โดยถือว่าเป็นเรื่องที่เกี่ยวข้องกับเสรีภาพและความกินดีอยู่ดี ที่ผ่านมาสหรัฐฯ ได้ตั้งคณะทำงานขึ้นเพื่อศึกษาและหาข้อเสนอแนะในการคุ้มครองข้อมูลส่วนตัวของประชาชนที่เกี่ยวข้องกับการสื่อสารด้วยอินเตอร์เนท ข้อเสนอดังกล่าวมีหลักการที่สำคัญสองประการ คือ หนึ่ง ผู้เก็บข้อมูลจะต้องแจ้งให้ผู้บริโภคทราบว่าจะเก็บข้อมูลอะไร และจะนำไปใช้เพื่อจุดประสงค์ใด สอง ผู้เก็บข้อมูลจะต้องเปิดโอกาสให้ผู้บริโภคสามารถเรียกร้องค่าเสียหายได้ในกรณีที่ถูกละเมิด และให้อนุญาตให้สามารถปกปิดชื่อในการใช้บริการการพาณิชย์อิเล็คทรอนิคส์ในบางกรณี

6. ความปลอดภัย (security) เครือข่ายการสื่อสารสำหรับการพาณิชย์อิเล็ค

ทรอนิคส์จะต้องมีความปลอดภัยจากการแอบดูหรือปลอมแปลงข้อมูล สหรัฐฯ สนับสนุนให้เกิดการพัฒนาบริการการรับรองที่เชื่อถือได้ที่จะช่วยให้คู่ค้าทราบว่า ตนกำลังทำการค้ากับใคร โดยใช้เทคโนโลยีการเข้ารหัส (Encryption) รัฐบาลสหรัฐฯ โดยความร่วมมือของภาคเอกชนกำลังจะร่วมกันพัฒนาโครงสร้างพื้นฐานของการสื่อสารโดยการเข้ารหัส โดยใช้กุญแจสาธารณะซึ่งสามารถกอบกู้กุญแจรหัสได้ กรณีที่เจ้าของทำหาย

7. โครงสร้างพื้นฐานทางโทรคมนาคม (Telecommunications Infrastructure) และเทคโนโลยีสารสนเทศ (Information Technology) ความสำเร็จของการพาณิชย์อิเล็คทรอนิคส์ในระดับโลกจะขึ้นอยู่กับโครงสร้างพื้นฐานทางโทรคมนาคม และอุปกรณ์ปลายทางที่เชื่อถือได้ สหรัฐฯ มีจุดยืนในการผลักดันให้รัฐบาลแต่ละประเทศ แปรรูปกิจการโทรคมนาคมของรัฐเป็นของเอกชน และส่งเสริมให้เกิดการแข่งขันในตลาดสายเช่า วงจรท้องถิ่น และอินเตอร์เนท

8. เนื้อหาของสารสนเทศในการคุ้มครองผู้บริโภคหรือเยาวชนจากสารสนเทศที่มีปัญหานั้น รัฐบาลสหรัฐฯ ต่อต้านการควบคุมสารสนเทศ แต่สนับสนุนการใช้การกำกับดูแลภายในเครือข่ายอินเตอร์เนทเอง เช่น การใช้การให้เรทติ้งในการกระตุ้นให้เกิดการสร้างสนเทศที่ดี หรือการใช้เทคโนโลยีใหม่ในการกรองหรือสกัดสารสนเทศที่ไม่เหมาะสม สหรัฐฯ ยังคัดค้านการจำกัดสัดส่วนเนื้อหาสารสนเทศจากต่างประเทศ

9. มาตรฐานทางเทคนิค สหรัฐฯ เชื่อว่ารัฐควรปล่อยให้ตลาดเป็นผู้กำหนดมาตรฐานของเทคนิคต่างๆ ในการเชื่อมต่อกันเอง เนื่องจากการเข้าไปกำหนดมาตรฐานของรัฐอาจเป็นอุปสรรคในการพัฒนาเทคโนโลยี ซึ่งมีการเปลี่ยนแปลงเร็วมาก นอกจากนี้ ประเทศต่างๆ จะต้องระวังไม่ให้มีการใช้มาตรฐานเป็นอุปสรรคกีดกันทางการค้า ทั้งนี้ ควรส่งเสริมให้เกิดมาตรฐานแบบสมัครใจและไม่จำเป็นต้องผลักดันให้มีมาตรฐานเดียวสำหรับเทคโนโลยีหนึ่งๆ [3]

เกี่ยวกับเรื่องความปลอดภัยบนอินเตอร์เนทเป็นปัญหาสำคัญอย่างยิ่งต่อการพาณิชย์อิเล็คทรอนิคส์ ทางการสหรัฐฯ ได้ประกาศที่จะทำให้พาณิชย์อิเล็คทรอนิคส์เป็นสถานที่สุดยอดปลอดภัยในการทำธุรกิจ โดยสั่งให้ FBI ประสานงานกับอัยการกลางทั่วประเทศตามล่า

---

[3] สมเกียรติ ตั้งกิจวานิชย์ , "การพาณิชย์อิเล็คทรอนิคส์ (ส่วนหนึ่งของโครงการแผนแม่บทกระทรวงพาณิชย์ พ.ศ.2540-2549)," กรุงเทพมหานคร : สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, 2541.

Hacker กวนเมืองที่ป่วนเว็บไซต์ยอดนิยมหลายต่อหลายแห่งมาดำเนินคดีให้จงได้ เจเน็ต เรโน รัฐมนตรียุติธรรมสหรัฐฯ แถลงว่า สำนักงานสอบสวนกลาง (FBI) จะเปิดการสอบสวนอย่างเต็มรูปแบบกรณีที่มีการโจมตีเว็บไซต์ยอดนิยมหลายแห่ง ซึ่ง ณ เวลานี้ไม่อาจล่วงรู้แรงจูงใจเบื้องหลังการโจมตีเหล่านี้ แต่ดูเหมือนว่าคนเหล่านั้นจะมีจุดประสงค์ในการรบกวนการค้าระบบอิเล็คทรอนิคส์ที่ถูกต้องตามกฎหมาย เว็บไซต์ที่ตกเป็นเป้าหมายของกลุ่มก่อกวนนี้ ได้แก่ Yahoo, Amazon.com, Ebay.com และ cnn.com นอกจากนั้น worldbestbuy.com ที่มีสำนักงานใหญ่ในซานดิเอโก เผยว่าเว็บไซต์ของบริษัทถูกเล่นงานทำให้บางส่วนของบริการอีคอมเมิร์ซหยุดชะงักเป็นเวลาหลายชั่วโมง ขณะที่เครือข่าย CNBC รายงานว่าเว็บไซต์ทางด้านการเงิน etrade.com ถูกโจมตีเช่นเดียวกัน บริษัทเหล่านี้เรียกปัญหานี้ว่า "การโจมตีแบบขอบริการลวง" เนื่องจาก Hacker ไม่ได้เจาะเข้ามาในระบบรักษาความปลอดภัยของพวกเขาแต่อย่างใด เพียงแต่ส่งข้อมูลปริมาณมหาศาลเข้ามาจนทำให้ผู้ใช้รายอื่นไม่สามารถเข้ามาในเว็บไซต์ได้ ปฏิบัติการของกลุ่ม Hacker กวนเมืองครั้งนี้ตอกย้ำถึงความสำคัญของพาณิชย์อิเล็คทรอนิคส์ที่มีต่อการขยายตัวทางเศรษฐกิจของสหรัฐฯ เนื่องจากเป้าหมายการโจมตีในระลอกแรกล้วนแต่เป็นเว็บไซต์ยอดนิยมทั้งสิ้น[4]

ศูนย์ป้องกันโครงสร้างพื้นฐานแห่งชาติ เรียกร้องให้บริษัทต่างๆ รวมถึงผู้บริโภคใช้โปรแกรมตรวจสอบว่า คอมพิวเตอร์ในการครอบครองถูกลักลอบติดตั้งเครื่องมือบางอย่างที่ Hacker ใช้ในการจู่โจมหรือไม่ ในส่วนของนายวิลเลียม ดาเล่ย์ รัฐมนตรีพาณิชย์ของสหรัฐกล่าวว่า การโจมตีที่เกิดขึ้นเป็นเสมือนเสียงปลุกวงการให้ตื่นขึ้นมารับรู้ถึงความอ่อนไหวของโครงสร้างระบบธุรกิจในเว็บซึ่งจะต้องมีการพัฒนาระบบความมั่นคงปลอดภัยให้มากขึ้น โดยกระทรวงพาณิชย์ได้สั่งให้มีการตรวจสอบระบบคอมพิวเตอร์ของหน่วยงานต่างๆ รวมทั้งคอมพิวเตอร์ของกระทรวงกลาโหมสหรัฐ และตามมหาวิทยาลัยต่างๆ ตลอดจนของบริษัทเอกชนให้มั่นใจได้ว่า จะไม่ถูกใช้เป็นฐานโจมตีบริการของเว็บไซต์ นอกจากนี้เจ้าหน้าที่ของกระทรวงยังได้ออกพบปะผู้บริหารของบริษัทยักษ์ใหญ่ 90 บริษัท ที่ติดอันดับบริษัทยักษ์ใหญ่ของนิตยสารฟอร์จูน 500 อันดับแรก เพื่อหารือถึงความพยายามร่วมมือกันป้องกันและต่อต้านการก่อการร้ายในระบบเว็บ นายดาเล่ย์ กล่าวอีกว่าจะมีการจัดตั้งคณะที่ปรึกษาของทำเนียบประธานาธิบดี จำนวน 30 คน เพื่อทำหน้าที่หามาตรการป้องกันความปลอดภัยในระบบเว็บไซต์อีกด้วย โดยใช้งบประมาณส่วนหนึ่งของงบประมาณลงทุนพัฒนาระบบป้องกันภัยในระบบคอมพิวเตอร์ ที่ตั้งไว้ถึง 2,000 ล้านเหรียญสหรัฐ สำหรับงบประมาณปี 2000 เป็นทุนดำเนินงานและโครงการต่างๆ นายโดนัลด์ ดิ๊ก ผู้

---

[4] หนังสือพิมพ์ผู้จัดการ ธุรกิจและการเงิน ปีที่ 10 ฉบับที่ 2862 (2860) วันศุกร์ที่ 11 กุมภาพันธ์ 2543 หน้า 17-19.

เชี่ยวชาญด้านอาชญากรรมคอมพิวเตอร์ของ FBI กล่าวว่า โทษสำหรับผู้ก่ออาชญากรรมในระบบอินเตอร์เนท นอกจากจะได้แก่โทษจำคุกสูงสุดนาน 5-10 ปี ปรับเป็นเงินอีก 250,000 ดอลลาร์ ยังอาจเพิ่มโทษนี้ได้อีกเท่าตัว ของค่าความเสียหายที่เกิดแก่เจ้าทุกข์[5]

กฎหมายของประเทศสหรัฐอเมริกา

1. The Credit Card Fraud Act of 1984[6]

เดิมประเทศสหรัฐอเมริกาใช้กฎหมายซึ่งแตกต่างกันหลายฉบับเพื่อดำเนินคดีกับการฉ้อโกงบัตรเครดิต เช่น มาตรา 1644 ของ Truth in Lending Act, กฎหมายเกี่ยวกับการฉ้อโกงทางไปรษณีย์ และกฎหมายการฉ้อโกงทางสื่อวิทยุหรือการสื่อสารแบบไร้สาย แต่มีกฎหมายเพียงฉบับเดียว คือ มาตรา 1644 ของ Truth in Lending Act ที่บัญญัติขึ้นเพื่อดำเนินการกับบัตรเครดิตเป็นกรณีพิเศษ อย่างไรก็ตาม กฎหมายฉบับนี้ถูกร่างขึ้นมาเพื่อส่งเสริมให้มีการใช้บัตรตามที่กำหนด ห้ามการใช้บัตรซึ่งผิดกฎหมายหรือรับสินค้าที่ซื้อด้วยบัตรที่ผิดกฎหมาย มิได้มีจุดประสงค์เพื่อลดการฉ้อโกงบัตรเครดิต กฎหมายฉบับนี้จึงมีปัญหาสำคัญที่เกิดขึ้น ได้แก่

1. หมายเลขบัตรเครดิต (Card Account/Card Number)

ปัจจุบันสิ่งที่คนร้ายต้องการไม่ใช่ตัวบัตรเครดิต แต่เป็นเพียงหมายเลขบัตรเท่านั้น เพราะคนร้ายสามารถนำหมายเลขบัตรไปใช้ในการฉ้อโกงได้หลายรูปแบบ แต่กฎหมายฉบับนี้ไม่มีบทบัญญัติห้ามการใช้หมายเลขบัตรโดยปราศจากอำนาจ (unauthorized account number) ดังที่บัญญัติว่า "ผู้ใดโดยเจตนา....ใช้บัตรเครดิตปลอม ปลอมลายมือ บัตรเครดิตที่สูญหาย หรือถูกลัก หรือบัตรเครดิตที่ได้มาโดยทุจริต...." ตามบทบัญญัติดังกล่าวมุ่งให้ความสำคัญเฉพาะตัวบัตรเครดิตเท่านั้น ดังนั้น การใช้เฉพาะหมายเลขบัตรเครดิตในการกระทำทุจริตจึงไม่เป็นความผิดตามกฎหมายนี้[7] ดังจะเห็นได้จากคดี United States v. Callihan ที่ผู้กระทำผิดติดต่อสื่อสารผ่านโทรศัพท์ระหว่างรัฐ โดยใช้หมายเลขบัตรเครดิตที่ได้มาโดยทุจริต ศาลตัดสินว่า "บัตร

---

[5] หนังสือพิมพ์มติชน ฉบับที่ 8009 วันศุกร์ที่ 11 กุมภาพันธ์ 2543 หน้าที่ 18.

[6] Title 18 United States Code Chapter 47 section 1029 Fraud and related activity in connection with access devices.

[7] จนิษฐ คันธสมบูรณ์ , "การทุจริตโดยใช้บัตรเครดิต ," (วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย . 2538) , หน้า 50.

เครดิต" ตามมาตรา 1644 ไม่ได้ขยายความไปถึงหมายเลขบัตรเครดิตด้วยเพราะไม่ใช่การใช้ตัวบัตร[8] หลังจากคดีนี้ผ่านพ้นไปหนึ่งปี เกิดคดีระหว่าง United States v. Bice-bey จำเลยได้สั่งซื้อสินค้าจากรัฐอื่นโดยใช้หมายเลขบัตรเครดิตของผู้อื่นโดยปราศจากอำนาจ ศาลได้พิจารณาว่าจำเลยต้องรับผิดตามมาตรา 1644 ฐานฉ้อโกงบัตรเครดิต ศาลได้ให้เหตุผลว่าหมายเลขบัตรเป็นส่วนสำคัญส่วนหนึ่งของบัตรเครดิต ดังนั้น การฉ้อโกงหมายเลขบัตรเครดิตจึงเป็นการฝ่าฝืนมาตรา 1644 แต่ความเห็นส่วนใหญ่ก็ยังคงเห็นด้วยกับคำจำกัดความของ The Ninth Circuit ว่า Truth in Lending Act กำหนดให้บัตรเครดิตเป็นสิ่งประดิษฐ์ชนิดหนึ่ง ด้วยเหตุนี้กฎหมายจึงไม่ห้ามการฉ้อโกงต่อหมายเลขบัตร เพราะหมายเลขบัตรเป็นเพียงนามธรรม (Intangible) ไม่ใช่สิ่งที่ประดิษฐ์ขึ้น ดังนั้น จึงเห็นว่าคำจำกัดความแคบๆ ของบัตรเครดิตตามกฎหมายนี้จึงเป็นช่องโหว่ขนาดใหญ่ของกฎหมาย

2. จำนวนรวมของการใช้บัตร (Aggregation)

มาตรา 1644 ห้ามการใช้บัตรเครดิตที่มีมูลค่ารวมกันตั้งแต่ 1,000 เหรียญสหรัฐต่อหนึ่งบัตรในระยะเวลาหนึ่งปี จึงมีข้อเท็จจริงที่ปรากฏให้เห็นอยู่ว่าเจ้าพนักงานของรัฐไม่อาจฟ้องร้องดำเนินคดีกับคนร้ายที่ใช้บัตรในมูลค่ารวมไม่ถึง 1,000 เหรียญสหรัฐ โดยคนร้ายมักจะทุจริตต่อบัตรเครดิตหลายใบแต่จะใช้อย่างระมัดระวังไม่ให้เกินวงเงิน 1,000 เหรียญสหรัฐต่อหนึ่งบัตร โดยเมื่อรวมความเสียหายที่เกิดขึ้นแล้วจะเป็นจำนวนเงินที่สูงเกินกว่า 1,000 เหรียญสหรัฐในรอบระยะเวลาหนึ่งปี[9]

จากปัญหาการบังคับใช้กฎหมายข้างต้น เป็นเหตุให้สภาของสหรัฐอเมริกาได้แก้ไขปรับปรุงกฎหมาย โดยในปี ค.ศ.1984 สภาคองเกรสได้ออกกฎหมาย The Credit Card Fraud Act of 1984 ขึ้น ซึ่งเป็นส่วนหนึ่งของ The Comprehensive Crime Control Act ทั้งนี้เพื่อแก้ไขข้อบกพร่องต่างๆ ในมาตรา 1644 ของ Truth in Lending Act โดยบัญญัติไว้ในบทที่ 18 มาตรา

---

[8] Melhem, Ahmed Al., "The Legal Regime of Payment Cards : A comparative Study between American, British and Kuwaiti Laws, With Particular Reference to Credit Cards ," (Ph.D.thesis The university of Exeter England 1990.), p.515.

[9] Caminer Brian F., "Comment, Credit Card Fraud : Neglected Crime", Journal of Criminal Law and Criminology ,Vol.76 No.18 (1965) : p. 746-763.

1029 [10] เรื่องการฉ้อโกงและการกระทำที่เกี่ยวข้องอันเกี่ยวกับเครื่องมือเชื่อมต่อ (Fraud and Related activity in connection with access devices) กฎหมายฉบับนี้ได้กำหนดให้การใช้หมายเลขบัตรเครดิตโดยปราศจากตัวบัตร สามารถที่จะก่อให้เกิดความผิดฐานฉ้อโกงบัตรเครดิตได้ โดยได้ให้ความหมายของคำว่า "access device" ไว้ในข้อ (d) ว่าหมายถึง บัตร แผ่น รหัส หมายเลขบัญชี เลขที่ชุดอิเล็คทรอนิคส์ เลขหมายเฉพาะเคลื่อนที่ เลขที่ประจำตัวประชาชน บริการโทรคมนาคมอื่นๆ หรือสิ่งอื่นใดก็ตามที่สามารถใช้เข้าสู่บัญชี ซึ่งสามารถใช้ได้โดยตัวมันเองหรือใช้ร่วมกับ access device อื่นๆ เพื่อให้ได้รับมาซึ่งเงิน สินค้า หรือสิ่งอื่นใดที่มีมูลค่า หรือนำไปใช้เพื่อที่จะโอนเงิน

จากความหมายข้างต้นจะเห็นได้ว่า บทบัญญัตินี้มิได้มุ่งที่จะให้ความหมายเฉพาะของคำว่า "บัตรเครดิต" เท่านั้น แต่ได้ใช้คำว่า "access device" ซึ่งกำหนดความหมายไว้อย่างกว้างขวางโดยครอบคลุมถึงตัวบัตรเครดิต หมายเลขบัตรเครดิต และอุปกรณ์เชื่อมต่ออื่นด้วย อันสามารถนำไปปรับใช้กับการทุจริตต่อบัตรเครดิตในรูปแบบต่างๆ ก่อให้เกิดการบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพมากขึ้น นอกจากนี้ ยังห้ามการครอบครองบัตรเครดิตซึ่งผิดกฎหมายตั้งแต่ 15 บัตรขึ้นไป อันเป็นการช่วยแบ่งเบาภาระหน้าที่เจ้าพนักงานของรัฐในการพิสูจน์ความผิด และกรณีความเสียหายที่เกิดขึ้นจะถูกพิจารณาถึงมูลค่ารวมโดยไม่คำนึงถึงจำนวนบัตรเครดิตที่ถูกนำไปใช้ ทั้งนี้ เพื่อช่วยขจัดปัญหาเรื่อง Aggregation[11]

มาตรา 1029 นี้มิใช่สิ่งที่จะนำมาใช้แทนมาตรา 1644 แต่จะช่วยส่งเสริมสนับสนุนกฎหมายเกี่ยวกับการฉ้อโกงบัตรเครดิตที่กำลังใช้บังคับอยู่ มีการกำหนดโทษจำคุกและโทษปรับให้สูงขึ้น ทั้งนี้เพื่อป้องกันผลประโยชน์จากการสูญเสียและเพื่อป้องกันอาชญากรรมที่จะเกิดขึ้น โดย มาตราดังกล่าวได้วางหลักเกี่ยวกับการกระทำความผิดไว้ดังนี้

ข้อ (a)

1. โดยรู้อยู่และเจตนาที่จะฉ้อโกง ผลิต ใช้ หรือค้า access device ปลอมตั้งแต่หนึ่งชิ้นขึ้นไป

---

[10] 18 U.S.C., section 1029.

[11] Caminer Brian F., Journal of Criminal Law and Criminology ,Vol.76 No.18 (1965) : p. 759-760.

2. โดยรู้อยู่และเจตนาที่จะฉ้อโกง ค้า หรือใช้ access device ที่ไม่ได้รับอนุญาตหนึ่งชิ้นขึ้นไปในรอบระยะเวลา 1 ปี และโดยการกระทำเช่นว่านั้นไปได้ไปซึ่งสิ่งมีค่ารวมกันเป็นจำนวน 1,000 เหรียญสหรัฐขึ้นไปในรอบระยะเวลานั้น
3. โดยรู้อยู่และเจตนาที่จะฉ้อโกง ครอบครอง access device ซึ่งเป็น access device ปลอมหรือที่ไม่ได้รับอนุญาตจำนวนตั้งแต่ 15 ชิ้นขึ้นไป
4. โดยรู้อยู่และเจตนาที่จะฉ้อโกง ผลิต ค้า ควบคุม เก็บรักษาหรือครอบครองอุปกรณ์ผลิตเครื่องมือ
5. โดยรู้อยู่และเจตนาที่จะฉ้อโกง ก่อให้เกิดผลในการติดต่อซื้อขายโดยการใช้ access device หนึ่งชิ้นหรือมากกว่านั้นที่ออกให้กับบุคคลอีกคนหนึ่งหรือหลายคน เพื่อที่จะได้รับเงินหรือสิ่งมีค่าใดในระยะเวลา 1 ปี มีมูลค่ารวมทั้งสิ้นเท่ากับหรือมากกว่า 1,000 เหรียญสหรัฐ
6. โดยมิได้รับอนุญาตจากผู้ออก access device โดยรู้อยู่และเจตนาที่จะฉ้อโกง ชักชวนบุคคลหนึ่งโดยมีจุดประสงค์เพื่อ
    A. เสนอ access device หรือ
    B. ขายข้อมูลที่เกี่ยวกับ หรือวิธีการที่จะได้ไปซึ่ง access device
7. โดยรู้อยู่และโดยเจตนาฉ้อโกง ใช้ ผลิต ค้า ควบคุม เก็บรักษา หรือครอบครองเครื่องมือโทรคมนาคมซึ่งถูกปรับเปลี่ยน หรือแก้ไข เพื่อที่จะได้ไปซึ่งการใช้บริการโทรคมนาคมที่ไม่ได้รับอนุญาต
8. โดยรู้อยู่และเจตนาที่จะฉ้อโกง ใช้ ผลิต ค้า ควบคุม เก็บรักษา หรือครอบครองซึ่ง scanning receiver
9. โดยรู้อยู่ ใช้ ผลิต ค้า ควบคุม เก็บรักษา หรือครอบครองฮาร์ดแวร์หรือซอฟต์แวร์ โดยรู้ว่าได้ถูกสร้างขึ้นเพื่อที่จะบรรจุในหรือเปลี่ยนแปลงการโทรคมนาคมที่บ่งชี้ข้อมูลที่สัมพันธ์กับหรือบรรจุอยู่ในอุปกรณ์โทรคมนาคม เพื่อที่ว่าเครื่องมือเช่นว่านั้นอาจจะถูกใช้ในการได้ไปซึ่งบริการโทรคมนาคมที่ไม่ได้รับอนุญาต
10. โดยมิได้รับอนุญาตจากสมาชิกระบบบัตรเครดิตหรือตัวแทน โดยรู้อยู่และเจตนาที่จะฉ้อโกง เป็นเหตุให้หรือดำเนินการให้บุคคลอีกคนหนึ่งแสดงหลักฐานหรือบันทึกการติดต่อทางธุรกิจที่ถูกสร้างโดย access device หนึ่งชิ้นขึ้นไป ต่อสมาชิกหรือตัวแทนเพื่อการจ่ายเงิน ต้องระวางโทษตามที่บัญญัติไว้ในอนุมาตรา (c) ของมาตรานี้ ถ้าความผิดกระทบต่อการค้าระหว่างรัฐหรือต่างประเทศ

บทบัญญัติในมาตรานี้ได้กำหนดโทษสำหรับการกระทำความผิดข้างต้นไว้ใน ข้อ(c) ว่ากรณีความผิดที่ไม่ได้เกิดขึ้นหลังจากการลงโทษสำหรับความผิดอีกฐานหนึ่งตามมาตรานี้ หากความผิดนั้นได้ถูกกระทำตามวรรค 1, 2, 3, 6, 7 หรือ 10 ของอนุมาตรา (a) ต้องระวางโทษปรับตามบทนี้หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ หากความผิดได้ถูกกระทำตามวรรค 4, 5, 8 หรือ 9 ต้องระวางโทษปรับตามบทนี้ หรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ กรณีความผิดเกิดขึ้นหลังจากการลงโทษสำหรับความผิดอีกฐานหนึ่งตามมาตรานี้ ต้องระวางโทษปรับตามบทนี้ หรือจำคุกไม่เกินกว่า 20 ปี หรือทั้งจำทั้งปรับ และไม่ว่ากรณีใดก็ตาม ทรัพย์สินส่วนตัวใด ๆ ที่ถูกใช้หรือตั้งใจจะใช้ในการกระทำความผิดต้องถูกริบเป็นของสหรัฐอเมริกา

นอกจากนี้ยังกำหนดให้หน่วยงานลับของสหรัฐอเมริกา The United State Secret Service (U.S.S.S.) มีอำนาจสืบสวนความผิดตามมาตรานี้ นอกเหนือไปจากตัวแทนอื่น ซึ่งอำนาจของหน่วยงานลับดังกล่าวต้องถูกใช้ให้สอดคล้องกับข้อตกลงที่ได้กระทำโดยรัฐมนตรีว่าการกระทรวงการคลังและอัยการสูงสุด

สำหรับความผิดตามมาตรา 1029 (a) 3 กรณีที่ผู้กระทำผิดรู้อยู่และเจตนาที่จะฉ้อโกง โดยครอบครอง access device ปลอมหรือที่ไม่ได้รับอนุญาตจำนวนตั้งแต่ 15 ชิ้นขึ้นไปนั้น มีตัวอย่างคดีที่เกิดขึ้น ดังนี้

คดี "Hacker" เป็นคดีระหว่าง United States of America โจทก์ Andrew Miffleton จำเลย เป็นข้อเท็จจริงเกี่ยวกับจำเลยซึ่งเป็นผู้มีความรู้ความเชี่ยวชาญทางด้านคอมพิวเตอร์ ได้ทำการเจาะระบบ (hack) เข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต และมีรหัสผ่านคอมพิวเตอร์ของบริษัทอินเตอร์เนทในระดับที่สามารถเข้าสู่การควบคุมระบบคอมพิวเตอร์ได้ทั้งหมด ซึ่งจำเลยได้นำไปใช้ในการเข้าสู่ (access) ระบบคอมพิวเตอร์ทั่วประเทศโดยไม่ได้รับอนุญาต นอกจากนี้ จำเลยยังได้ครอบครอง access device โดยไม่ได้รับอนุญาต อันได้แก่ รหัสผ่านของผู้ให้บริการอินเตอร์เนทที่มีไว้สำหรับให้บริการบุคคลทั่วไป หมายเลขประจำตัวเครื่องหรือหมายเลขสำหรับใช้บริการโทรศัพท์ในระบบ cellular หมายเลขบัตรโทรศัพท์เพื่อใช้ในการโทรศัพท์ทางไกล และหมายเลขบัตรเครดิต ดังนั้น ศาล US District Court , District of Texas จึงได้ตัดสินว่าจำเลยมีความผิดตามมาตรานี้[12]

---

[12] ข้อมูลดังกล่าวแปลมาจาก Hacker ใน Http://www.usdoj.gov (12 July 2001).

เกี่ยวกับความผิดฐานครอบครอง Access device มากกว่า 15 ชิ้นขึ้นไปนี้ มีข้อสังเกตจากคดี United State v. Russell, 908 F.2d 405 (8th Cir.1990) ซึ่งจำเลยครอบครองบัตรเครดิตที่ถูกขโมยมาในหลายโอกาส แต่ไม่มีครั้งใดที่จำเลยครอบครอง Access device มากกว่า 15 ชิ้นขึ้นไปในเวลาเดียวกัน จำเลยจึงถูกตัดสินว่าไม่มีความผิดตามมาตรานี้ [13]

2. Identity Theft and Assumption Deterrence Act of 1998[14]

ในสังคมปัจจุบัน การใช้ข้อมูลส่วนบุคคลชนิดต่างๆ อันได้แก่ ข้อมูลหมายเลขบัตรเครดิต ชื่อ ที่อยู่ เบอร์โทรศัพท์ หมายเลขใบอนุญาตขับขี่ หรือหมายเลขประกันสังคม Social Security Number (SSN) เป็นสิ่งสำคัญอย่างยิ่งในชีวิตประจำวัน ไม่ว่าเพื่อการซื้อขายสินค้าและบริการ การสมัครงาน หรือการทำสัญญา เป็นต้น แต่ในขณะที่มีการส่งผ่านและการใช้ข้อมูลส่วนบุคคลดังกล่าวนี้อาจมีคนร้ายแอบขโมยหรือสักลอบนำข้อมูลไปใช้แสวงหาประโยชน์โดยมิชอบ ซึ่งการกระทำในลักษณะนี้ถูกเรียกว่า "Identity Theft"

รูปแบบหนึ่งของการกระทำความผิดดังกล่าวข้างต้น คือ การขโมยหมายเลขบัตรเครดิตของผู้อื่นเพื่อนำไปใช้ในการสั่งซื้อสินค้าและบริการบนอินเตอร์เนทโดยทุจริต หรือหากเป็นข้อมูลอย่างอื่นที่มิใช่หมายเลขบัตรเครดิต คนร้ายอาจนำไปใช้ในการยื่นสมัครขอทำบัตรเครดิตจากสถาบันผู้ออกบัตร และนำบัตรเครดิตนั้นไปใช้แสวงหาประโยชน์โดยมิชอบต่อไป โดยผู้ที่ได้รับความเสียหายก็คือเจ้าของข้อมูลหรือเจ้าของบัตรเครดิตที่แท้จริงนั่นเอง การป้องกันอย่างสมบูรณ์แบบเพื่อมิให้ตกเป็นเหยื่อของอาชญากรรมประเภทนี้เป็นเรื่องที่ไม่น่าจะเป็นไปได้ แต่สามารถลดความเสี่ยงที่จะเกิดขึ้นได้โดยการจัดการกับข้อมูลส่วนบุคคลของแต่ละคนอย่างรอบคอบและระมัดระวัง[15]

---

[13] ข้อมูลดังกล่าวแปลมาจาก Credit card Fraud in the late 90's ใน Http://www.into-sec.com/commerce/ commerce_012798 a.html-ssi, (20 May 2001).

[14] Title 18 United States Code Chapter 47 section 1028 Fraud and Related Activity in Connection with Identification Documents and Information.

[15] ข้อมูลดังกล่าวแปลมาจาก ID Theft : When Bad Things Happen To Your Good Name ใน Http://www.ftc. gov/bcp/ conline/pubs/ credit/idtheft.htm , (20 May 2001).

วิธีการได้มาซึ่งข้อมูลส่วนบุคคลของผู้อื่น ได้แก่

- ขโมยกระเป๋าสตางค์ซึ่งภายในจะบรรจุบัตรเครดิตหรือบัตรประจำตัวของผู้นั้นไว้ ค้นหาสลิป (Slip) บัตรเครดิตหรือใบสมัครขอทำบัตรเครดิตซึ่งยังไม่ถูกฉีกทำลายจากถังขยะ
- ขโมยข้อมูลจากระบบคอมพิวเตอร์ รวมถึงบนเครือข่ายอินเตอร์เนท
- จัดตั้งเว็บไซต์เกี่ยวกับ E-commerce ขึ้นเพื่อหลอกลวงให้ได้มาซึ่งหมายเลขบัตรเครดิตของผู้อื่นที่หลงเชื่อเข้ามาสั่งซื้อสินค้าและบริการ โดยที่เว็บไซต์ดังกล่าวมิได้มีวัตถุประสงค์อย่างแท้จริงในการทำ E-commerce กับบุคคลทั่วไป
- แจ้งเปลี่ยนที่อยู่ในการจัดส่งเอกสารต่างๆ ของเจ้าของข้อมูลที่แท้จริงไปยังที่อยู่แห่งใหม่ที่คนร้ายต้องการ
- ใช้อุบายหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลจากหน่วยงานต่างๆ ที่เก็บรักษาหรือมีสิทธิได้ข้อมูลมาโดยถูกต้องตามกฎหมาย
- ซื้อข้อมูลจากพนักงานหรือลูกจ้างของร้านค้า ปั๊มน้ำมัน หรือสถานีบริการอื่นๆ

สิ่งที่เลวร้ายที่สุดในการจัดการกับอาชญากรรมทุกชนิดที่เกิดขึ้น คือ การที่รู้ตัวผู้กระทำผิดแต่กลับไม่มีกฎหมายใดสามารถลงโทษผู้นั้น รวมถึงหาทางเยียวยาเหยื่อผู้เคราะห์ร้ายให้ได้รับการชดใช้ที่เหมาะสมได้ แต่เดิมนั้นกฎหมายที่ใช้บังคับอยู่ได้กำหนดความผิดสำหรับการใช้เอกสารส่วนบุคคลอันเป็นเท็จโดยมิชอบ (Misuse of False Identification Documents) เท่านั้น คำว่า "เอกสาร" หมายถึง ตัวเอกสารจริงๆ แต่ด้วยความเจริญก้าวหน้าทางด้านเทคโนโลยี ทำให้ข้อมูลส่วนบุคคลสามารถถูกพบได้บนเครือข่ายอินเตอร์เนท ผู้ที่จะขโมยข้อมูลไม่จำเป็นต้องใช้เอกสารที่แท้จริง เพราะเขาสามารถเข้าสู่ระบบออนไลน์เพื่อค้นหาข้อมูลเหล่านั้นได้ ไม่ว่าจะเป็น ชื่อ ที่อยู่ เบอร์โทรศัพท์ หรือหมายเลขบัตรเครดิต เป็นต้น ด้วยเหตุนี้การคุ้มครองข้อมูลส่วนบุคคลจึงเป็นเรื่องที่มีความสำคัญอย่างยิ่ง ดังนั้น เมื่อวันที่ 30 ตุลาคม ค.ศ.1998 รัฐสภาของสหรัฐอเมริกาจึงบัญญัติ Identity Theft and Assumption Deterrence Act of 1998 ขึ้นมาเพื่อใช้บังคับกับการกระทำความผิดในลักษณะดังกล่าว โดยกำหนดให้ Identity Theft เป็นอาชญากรรมประเภท Federal Crime มีโทษจำคุกขั้นสูงถึง 15 ปี และปรับสูงสุดเป็นจำนวน 250,000 เหรียญสหรัฐ นอกจากนี้ยังจัดให้ Federal Trade Commission (FTC) เป็นหน่วยงาน (Clearing House) เพื่อให้ความช่วยเหลือผู้ซึ่งตกเป็นเหยื่อ โดยการชี้แจงแก้ไขบันทึกทางด้านเครดิตของเหยื่อ เพราะเหยื่อของอาชญากรรมประเภทนี้มักจะถูกรายงานทางเครดิตในด้านลบจากสถาบันการเงินหรือ

สถาบันผู้ออกบัตรเครดิตที่เกี่ยวข้อง และกำหนดให้เหยื่อได้รับการชดใช้ค่าเสียหายจากผู้กระทำผิดด้วย[16]

กฎหมายฉบับนี้ได้จำกัดความหมายของคำสำคัญต่างๆ ที่เกี่ยวข้องและกำหนดลักษณะของการกระทำผิดไว้ ดังนี้

1. *เครื่องมือทำเอกสาร (Document-making Implement)* หมายถึง เครื่องมือใดๆ เครื่องพิมพ์ อุปกรณ์ อิเล็คทรอนิคส์ หรือคอมพิวเตอร์ฮาร์ดแวร์หรือซอฟต์แวร์ที่ถูกประกอบเป็นการเฉพาะหรือถูกใช้แต่แรกเพื่อทำเอกสารเฉพาะบุคคล เอกสารเฉพาะบุคคลปลอม หรือเครื่องมือทำเอกสารอีกอันหนึ่ง

2. *เอกสารส่วนบุคคล (Identification document)* หมายถึง เอกสารที่ถูกทำขึ้นหรือออกโดยหรือภายใต้อำนาจของรัฐบาลสหรัฐอเมริกา รัฐ หน่วยงานที่เกี่ยวกับการปกครองของรัฐ รัฐบาลต่างประเทศ รัฐบาลระหว่างประเทศ หรือองค์กรกึ่งรัฐบาลระหว่างประเทศ ซึ่งเมื่อได้รวมกับข้อมูลที่เกี่ยวข้องกับสิ่งใดโดยเฉพาะแล้ว ถือเป็นชนิดที่ถูกยอมรับโดยทั่วไปเพื่อจุดประสงค์แห่งการบ่งชี้เฉพาะของแต่ละบุคคล

3. *ลักษณะของความเฉพาะบุคคล (Means of Identification)* หมายถึง ชื่อหรือตัวเลขใดๆ ที่อาจจะถูกใช้เพียงลำพังหรือโดยสัมพันธ์กับข้อมูลอื่นใด เพื่อที่จะบ่งชี้ความเฉพาะของบุคคลนั้น ซึ่งรวมถึง
   A. ชื่อ เลขประกันสังคม (SSN) วันเกิด ใบอนุญาตขับขี่ที่ออกโดยรัฐบาล หรือหมายเลขประจำตัวประชาชน เลขทะเบียนคนต่างด้าว เลขหนังสือเดินทางรัฐบาล เลขประจำตัวลูกจ้างหรือผู้เสียภาษี
   B. ข้อมูลทางสถิติเกี่ยวกับชีววิทยาที่เป็นการเฉพาะ เช่น รอยพิมพ์นิ้วมือ เสียง เยื่อชั้นในที่รับภาพจากแล้วตา หรือภาพม่านตา หรือการแสดงออกทางกายภาพที่เป็นการเฉพาะ
   C. ตัวเลขอิเล็คทรอนิคส์ที่เป็นการเฉพาะ ที่อยู่ หรือรหัสผ่านหรือ

---

[16] ข้อมูลดังกล่าวแปลมาจาก Identity Theft and Assumption Deterrence Act of 1998 ใน Http://www.house.gov. bemie/statements/ 1998-10-07_idtheft.html, (20 May 2001).

D. ข้อมูลที่บ่งชี้การโทรคมนาคม หรือ access device ตามความหมายที่ให้ไว้ในมาตรา 1029

ลักษณะของการกระทำความผิดได้ถูกกำหนดไว้หลายรูปแบบดังนี้[17]

ข้อ (a) ผู้ใด

1. โดยรู้อยู่และปราศจากอำนาจตามกฎหมาย ได้ผลิตเอกสารส่วนบุคคลหรือเอกสารส่วนบุคคลปลอม
2. โยกย้ายเอกสารส่วนบุคคล หรือเอกสารส่วนบุคคลปลอม โดยรู้ว่าเอกสารนั้นถูกลักมาหรือถูกผลิตขึ้นโดยปราศจากอำนาจตามกฎหมาย
3. ครอบครองโดยเจตนาที่จะใช้หรือโยกย้ายอย่างผิดกฎหมายซึ่งเอกสารส่วนบุคคล หรือเอกสารส่วนบุคคลปลอมจำนวนห้าฉบับขึ้นไป (นอกเหนือไปจากเอกสารที่ออกโดยถูกกฎหมายเพื่อการใช้ของผู้ครองครอง)
4. ครอบครองเอกสารส่วนบุคคล หรือเอกสารส่วนบุคคลปลอม โดยเจตนาให้เอกสารเช่นว่านั้นถูกใช้เพื่อการฉ้อโกงสหรัฐอเมริกา
5. ผลิต โยกย้าย หรือครอบครองเครื่องมือทำเอกสาร โดยเจตนาให้เครื่องมือทำเอกสารเช่นว่านั้นถูกใช้ในการทำเอกสารส่วนบุคคลปลอม หรือเครื่องมือทำเอกสารอีกอันหนึ่งซึ่งจะถูกใช้เพื่อการนั้น
6. ครอบครองเอกสารส่วนบุคคลของสหรัฐอเมริกาโดยรู้ว่าถูกลักมาหรือถูกผลิตโดยปราศจากอำนาจตามกฎหมาย
7. โยกย้ายหรือใช้ Means of Identification ของผู้อื่นโดยปราศจากอำนาจตามกฎหมาย โดยเจตนาที่จะกระทำ หรือช่วย หรือยุยงการกระทำใดที่ผิดกฎหมาย ซึ่งเป็นการฝ่าฝืนกฎหมายของสหพันธรัฐ หรือทำให้เป็นความผิดอาญาภายใต้กฎหมายท้องถิ่นหรือของรัฐซึ่งใช้บังคับ

กฎหมายฉบับนี้ได้กำหนดโทษสำหรับการกระทำผิดข้างต้นไว้ว่าผู้กระทำผิดต้องระวางโทษปรับ หรือจำคุกไม่เกิน 15 ปี หรือทั้งจำทั้งปรับ ในกรณีความผิดเกี่ยวกับการผลิตหรือโยกย้ายเอกสารส่วนบุคคลหรือเอกสารส่วนบุคคลปลอม หากปรากฏว่าเป็นเอกสารที่ออกโดยหรือ

---

[17] 18 U.S.C. section 1028.

ภายใต้อำนาจของรัฐบาลสหรัฐอเมริกา หรือเอกสารเกี่ยวกับสูติบัตร ใบอนุญาตขับขี่ หรือบัตรประจำตัวประชาชน, การผลิตเอกสารส่วนบุคคลมากกว่า 5 ชิ้นขึ้นไป, การกระทำผิดตาม (a) 5 และการกระทำผิดตาม(a) 7 ที่เกี่ยวกับการโยกย้ายหรือการใช้ลักษณะเฉพาะบุคคล (รวมถึง access device ตามความหมายของ Means of Identification ด้วย) ตั้งแต่หนึ่งครั้งขึ้นไป ถ้าผลของความผิดทำให้บุคคลนั้นได้มาซึ่งสิ่งใดที่มีค่ารวมกันตั้งแต่ 1,000 เหรียญสหรัฐขึ้นไปในระยะเวลา 1 ปี

หากความผิดได้ถูกกระทำขึ้นเพื่อให้เกิดความสะดวกในการกระทำผิดอาญาฐานค้ายาเสพติดหรือฐานประทุษร้าย ต้องระวางโทษปรับ หรือจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ และหากความผิดได้ถูกกระทำขึ้นเพื่อให้เกิดความสะดวกในการกระทำความผิดฐานก่อการร้ายระหว่างประเทศต้องระวางโทษปรับ หรือจำคุกไม่เกิน 25 ปี หรือทั้งจำทั้งปรับ สำหรับความผิดนอกเหนือจากนี้ต้องระวางโทษปรับ หรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ นอกจากนี้ บุคคลใดที่พยายามหรือสมคบกันกระทำความผิด ต้องระวางเช่นเดียวกับโทษที่บัญญัติสำหรับความผิดนั้น

ทรัพย์สินที่ถูกใช้หรือมีไว้เพื่อใช้ในการกระทำผิดให้ถูกริบตกเป็นของสหรัฐอเมริกา และกำหนดให้ตัวแทนที่บังคับการให้เป็นไปตามกฎหมายของสหรัฐอเมริกา รัฐ หรือหน่วยงานทางการปกครองของรัฐ หรือตัวแทนลับของสหรัฐอเมริกาที่ได้รับมอบอำนาจตามกฎหมาย ให้มีอำนาจในการสืบสวนและการป้องกัน รวมทั้งดำเนินการที่เป็นความลับ

สำหรับเจ้าของข้อมูลที่ตกเป็นเหยื่อของอาชญากรรมประเภทนี้ สามารถร้องเรียนไปยัง Federal Trade Commission (FTC) ซึ่งเป็นหน่วยงานที่สภาของสหรัฐอเมริกากำหนดให้เป็นผู้จัดหาข้อมูลเกี่ยวกับ Identity Theft ให้แก่ผู้บริโภค และรับเรื่องราวร้องทุกข์ที่เกิดขึ้น แม้ว่า FTC จะไม่มีอำนาจนำเรื่องดังกล่าวเป็นสู่การดำเนินคดีทางอาญา แต่ก็สามารถจัดหาข้อมูลต่างๆ เพื่อช่วยเหลือและแก้ไขปัญหาให้แก่ผู้ที่ตกเป็นเหยื่อ ไม่ว่าจะเป็นปัญหาทางด้านการเงินหรือปัญหาอื่นใดก็ตามซึ่งเป็นผลจากอาชญากรรมนี้ โดย FTC จะเก็บรักษาข้อมูลของเหยื่อให้เป็นความลับ แต่ FTC อาจจัดส่งข้อมูลของเหยื่อไปยังหน่วยงานของรัฐหรือเอกชนที่เกี่ยวข้องเมื่อได้รับความยินยอมจากเหยื่อ ทั้งนี้ เพื่อจัดหาหน่วยงานหรือองค์กรที่เหมาะสมให้เข้ามาดำเนินการให้เกิดผลคืบหน้ามากยิ่งขึ้นต่อไป[18]

---

[18] ข้อมูลดังกล่าวแปลมาจาก Federal Trade Commission ใน Http://www.ftc.gov, (20 May 2001).

คดีที่เกี่ยวข้องกับการทุจริตต่อบัตรเครดิตซึ่งผู้กระทำถูกลงโทษตามกฎหมายนี้ ได้แก่ คดีของ Oliver Alaefule อายุ 31 ปี Charles Timothy อายุ 31 ปี และ Ifeany Onwuazo อายุ 24 ปี จำเลยทั้งสามร่วมกันขโมยข้อมูลส่วนบุคคลของผู้อื่น เช่น ชื่อ, วันเดือนปีเกิด, หมายเลขประกันสังคม เป็นต้น จากนั้นได้นำไปยื่นสมัครขอทำบัตรเครดิตในนามของผู้อื่นตามที่ได้ข้อมูลมา Timothy ขโมยข้อมูลต่างๆ ขณะที่เขาทำงานอยู่กับบริษัทตัวแทนให้เช่ารถภายในสนามบิน Sacramentro ระหว่างปี ค.ศ.1996-1998 เมื่อพวกเขาได้รับบัตรเครดิตแล้ว เขาได้นำไปใช้ซื้อสินค้าและบริการรวมถึงเบิกถอนเงินสดล่วงหน้า จำเลยทั้งสามได้ยื่นคำขอสมัครบัตรเครดิตเป็นจำนวนกว่า 100 ฉบับ ส่งผลให้บริษัทผู้ออกบัตรจัดทำบันทึกทางด้านเครดิตในทางลบต่อเจ้าของข้อมูลที่แท้จริง นอกจากนี้ พวกเขายังได้ขอเปิดตู้รับไปรษณีย์ (Mail Boxes) กว่า 20 แห่งภายในเมืองและรอบๆ เมือง Sacramentro ทั้งนี้เพื่อให้ยากแก่การสะกดรอยการกระทำผิดของพวกเขา ศาล Federal District Court โดยผู้พิพากษา Garland E.Burrell ได้ตัดสินจำคุก Oliver Alaefule เป็นเวลา 15 เดือน จำคุก Charles Timothy เป็นเวลา 31 เดือน และจำคุก Ifeany Onwuazo เป็นเวลา 12 เดือน [19]

คดีของ Robert Christopher Lawrence อายุ 37 ปี เมื่อวันที่ 5 กุมภาพันธ์ 2544 จำเลยสารภาพว่าได้รับและใช้บัตรเครดิตจากการนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้โดยทุจริต จำเลยเป็นลูกจ้างและทำงานอยู่ที่ Kaiser Permanente งานส่วนหนึ่งของเขาทำให้เขาสามารถเข้าถึงเอกสารทางด้านการแพทย์ซึ่งจะบันทึกข้อมูลส่วนบุคคลต่างของผู้ป่วย เช่น ชื่อ, วันเดือนปีเกิด, ที่อยู่ เป็นต้น เขารับสารภาพว่าเขาจะเลือกใช้เฉพาะข้อมูลของผู้ป่วยที่มีชื่อคล้ายกับเขา ทั้งนี้เพื่อนำไปยื่นขอบัตรเครดิต ศาล U.S. District Court, District of Maryland โดยผู้พิพากษา Peter J.Messitte ได้ตัดสินจำคุกจำเลยเป็นเวลา 33 เดือน คุมประพฤติเป็นเวลา 3 ปีภายหลังพ้นโทษ และชดใช้เงินจำนวน 78,672.67 เหรียญสหรัฐ[20]

---

[19] ข้อมูลดังกล่าวแปลมาจาก Final conspirator sentenced in credit card fraud ring ใน Http://www.consumer.gov/ idtheft/cases.htm,(3 November 2001).

[20] Ibid.

3. The Computer Fraud and Abuse Act of 1986[21]

เนื่องจากคอมพิวเตอร์เป็นศูนย์กลางของธุรกิจ การเมือง และการปกครอง ดังนั้น ความสนใจต่ออาชญากรรมทางคอมพิวเตอร์จึงเพิ่มขึ้นอย่างมากในช่วงต้นปี ค.ศ.1980 The Computer fraud and abuse Act of 1986 (CFAA) จึงถูกผลักดันให้เป็นกฎหมายเพื่อแก้ไขเปลี่ยนแปลงกฎหมายในปี 1984 ซึ่งได้รับการพิสูจน์แล้วว่าไม่สามารถจัดการกับปัญหาอาชญากรรมคอมพิวเตอร์ได้ CFAA เป็นผลงานจากการค้นคว้าและอภิปรายของผู้ร่างกฎหมายเป็นเวลาหลายปี สาเหตุหนึ่งของการร่างกฎหมายที่ยาวนานและเป็นสาเหตุที่สำคัญที่สุดก็คือ ความยากลำบากในการรวบรวมการให้ปากคำอย่างจริงจังของผู้เสียหาย เนื่องจากหลายบริษัทไม่เต็มใจที่จะยอมรับว่าตนเป็นผู้เสียหายเพราะพวกเขาเกรงว่าอาจเกิดความเสียหายได้หากมีการเปิดเผยเรื่องที่เกิดขึ้นต่อสาธารณชน ผู้ร่างกฎหมายคาดหวังว่าผู้เสียหายจะยอมปรากฏตัวมากขึ้นเมื่อกฎหมายและบทกำหนดโทษที่ชัดเจนได้ถูกจัดวางเข้าที่แล้ว CFAA ได้ทำให้ Fraud and Abuse Act ซึ่งเป็นกฎหมายที่บัญญัติขึ้นเมื่อปี ค.ศ.1984 ถูกพัฒนาให้รัดกุมยิ่งขึ้น และทำให้ The Electronic Communication Privacy Act of 1986 (ECPA) สมบูรณ์ขึ้น ดังนั้น เมื่อประธานาธิบดี Ronald Reagan ลงนามกฎหมาย CFAA ในวันที่ 16 ตุลาคม 1986 กฎหมายฉบับนี้จึงได้รับการสนับสนุนอย่างมากจากรัฐสภา รวมทั้งกระทรวงยุติธรรม[22]

กฎหมายฉบับนี้ได้แก้ไขบทที่ 18 ของกฎหมายสหรัฐมาตรา 1030 มีการเพิ่มบทลงโทษสำหรับการ "เข้าถึง" (Access) ระบบคอมพิวเตอร์ที่เกี่ยวข้องกับรัฐบาลกลาง (Federal interest computers) และกฎหมายฉบับนี้ยังสร้างความชัดเจนให้กับเรื่องการฉ้อโกงและการทุจริตทางคอมพิวเตอร์ ซึ่งเป็นการกระทำความผิดทางอาญาต่อคอมพิวเตอร์ของรัฐบาลกลาง เพื่อทำให้ความคลุมเครือทางกฎหมายและอุปสรรคในการดำเนินคดีหมดไป โดยถือว่ากิจกรรมทางคอมพิวเตอร์ 6 ประการต่อไปนี้เป็นอาชญากรรม

1. การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเพื่อนำเอาข้อมูลที่เป็นความลับของชาติไป โดยมีเจตนาที่จะทำให้เกิดความเสียหายต่อสหรัฐอเมริกา

---

[21] Title 18 United States Code Chapter 47 Section 1029 Fraud and related activity in connection with computers.

[22] ข้อมูลดังกล่าวแปลมาจาก Computer Fraud ใน Http://www.digitalcentury.com/encyclo/update/comfraud. html, (3 November 2000).

2. การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเพื่อเอาข้อมูลทางการเงินที่ได้รับการคุ้มครอง หรือข้อมูลเกี่ยวกับเครดิต

3. การเข้าถึงระบบคอมพิวเตอร์ของรัฐบาลกลางโดยไม่ได้รับอนุญาต

4. การเข้าถึงระบบคอมพิวเตอร์ซึ่งเป็นการข้ามรัฐข้ามประเทศโดยไม่ได้รับอนุญาต โดยจุดประสงค์เพื่อกระทำความผิด

5. การเข้าถึงระบบคอมพิวเตอร์ซึ่งเป็นการข้ามรัฐข้ามประเทศโดยไม่ได้รับอนุญาต และทำให้เกิดความเสียหายรวมตั้งแต่ 1,000 เหรียญสหรัฐขึ้นไป

6. การลักลอบขนย้าย แจกจ่ายรหัสผ่านระบบการเข้าถึงระบบคอมพิวเตอร์ เพื่อผลทางการค้าระหว่างรัฐ

รัฐบาลต้องพิสูจน์ว่ามีการเข้าไปในระบบคอมพิวเตอร์ที่เกี่ยวข้องกับรัฐบาลกลางโดยเจตนาเพื่อที่จะดำเนินคดีกับการกระทำผิดเหล่านี้ คำว่า "ระบบคอมพิวเตอร์ของรัฐบาลกลาง" หมายความรวมถึง คอมพิวเตอร์ที่รัฐบาลกลางเป็นเจ้าของ ที่รัฐบาลกลางใช้งาน และระบบคอมพิวเตอร์ที่มีคอมพิวเตอร์อย่างน้อยหนึ่งเครื่องถูกใช้ในการประกอบอาชญากรรม ซึ่งไม่จำเป็นต้องอยู่ในรัฐเดียวกัน นอกจากนี้ยังต้องมีหลักฐานว่าผู้กระทำผิดนั้นเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือเข้าถึงเพื่อการฉ้อโกง จากการที่กฎหมายมุ่งเน้นวิธีการที่คนร้าย *เข้าถึง* ระบบคอมพิวเตอร์มากกว่าวิธีการที่คนร้าย *ใช้* ระบบคอมพิวเตอร์ ทำให้การกระทำหลายๆ อย่างที่อาจจะเป็นอาชญากรรมนั้นถูกตัดออกไป เช่น การขโมยข้อมูลจากบริษัท หรือบุคคลภายในองค์กรของรัฐ หรือจากการกระทำของบุคคลที่ไม่ชัดเจนว่าได้รับอนุญาตหรือไม่ ซึ่งอาจจะไม่ถูกลงโทษตามหลักการนี้ หรือในกรณีที่บุคคลซึ่งได้รับอนุญาตให้ใช้ระบบคอมพิวเตอร์ แต่ว่าได้ทำการเปลี่ยนแปลง ทำให้เกิดความเสียหาย หรือทำลายข้อมูลที่อยู่ในระบบนั้น ก็อาจจะไม่ถูกลงโทษเช่นกัน การบังคับใช้กฎหมายฉบับนี้ในช่วงแรกๆ นั้น ไม่ต้องการให้มีการดำเนินคดีกับการเข้าถึงระบบคอมพิวเตอร์โดยปกติ เพราะเห็นว่าเป็นเพียงการใช้คอมพิวเตอร์และเข้าไปดูข้อมูลโดยไม่ได้รับอนุญาตเท่านั้น ไม่ถือเป็นอาชญากรรม[23]

กรณีการใช้กฎหมายฉบับนี้ที่โด่งดังที่สุดคือในปี 1989 ในการดำเนินคดีกับ Robert Tappan Morris ซึ่งเป็นนักศึกษามหาวิทยาลัยคอร์แนล Morris เป็นผู้สร้างโปรแกรม worm (ไวรัสคอมพิวเตอร์ชนิดหนึ่ง) ซึ่งถูกออกแบบมาให้แพร่กระจายไปทั่วเครือข่ายอินเตอร์เนท

---

[23] ข้อมูลดังกล่าวแปลมาจาก Criminal Law and the Internet ใน Http://www.cla.org/ruhbook/ chp11.htm, (3 November 2000).

เพื่อก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ที่มีระบบรักษาความปลอดภัยที่อ่อนแอ โปรแกรม worm ได้แพร่กระจายออกไปบนระบบคอมพิวเตอร์กว่า 6,000 ระบบ เป็นเหตุให้บริษัทต่างๆ ต้องเสียเวลาในการตรวจสอบและปรับปรุงระบบคอมพิวเตอร์ของตนเป็นเวลาหลายวัน ส่งผลให้เสียค่าใช้จ่ายในการดำเนินการหลายล้านเหรียญสหรัฐ Morris ต่อสู้คดีว่าเขาได้รับอนุญาตให้สามารถส่ง e-mail ถึงผู้ใช้รายอื่นบนเครือข่ายอินเตอร์เนทได้ ซึ่งทำให้เขาเป็น "ผู้ที่ได้รับอนุญาตให้ใช้และเข้าถึง" คอมพิวเตอร์เหล่านั้น แต่ศาลไม่รับฟังข้อต่อสู้ของจำเลย โดยศาลตัดสินให้คุมประพฤติจำเลยเป็นเวลา 3 ปี ทำประโยชน์ให้สังคมเป็นเวลา 400 ชั่วโมง และปรับเป็นเงิน 10,000 เหรียญสหรัฐ ซึ่งหลายคนวิจารณ์ว่าโทษดังกล่าวน้อยเกินไปสำหรับความเสียหายที่เกิดขึ้น ดังนั้นในเดือนกันยายน 1994 กฎหมายฉบับนี้จึงได้รับการแก้ไขอีกครั้งหนึ่ง เพื่อให้สามารถจัดการกับ "ไวรัสคอมพิวเตอร์" และโปรแกรมอื่นที่ถูกออกแบบมาเพื่อสร้างความเสียหาย หรือทำลายระบบคอมพิวเตอร์ เนื่องจากกฎหมายเก่านั้นมุ่งเน้นที่การได้รับอนุญาตของผู้กระทำผิดในการที่จะเข้าถึงระบบคอมพิวเตอร์นั้น จึงเป็นอุปสรรคในการแก้ปัญหาว่าการกระทำอาชญากรรมใดที่สามารถทำได้โดยไม่ต้อง "เข้าถึง" คอมพิวเตอร์ที่ได้รับความเสียหาย นอกจากนี้ยังลงโทษผู้กระทำผิดที่กระทำโดยไม่ยั้งคิดและไม่คำนึงถึงความเสี่ยงที่จะเกิดขึ้น และได้สร้างเสียหายให้เกิดขึ้น ซึ่งอาจถูกฟ้องร้องทางแพ่งจากผู้ที่ได้รับความเสียหายได้

CFAA ถูกร่างขึ้นมาในช่วงเวลาเดียวกับ 18 U.S.C. sec1029 ซึ่งเป็นกฎหมายที่เกี่ยวกับการฉ้อโกงบัตรเครดิตและมีองค์ประกอบคล้ายๆ กับการกระทำฉ้อโกงอื่นๆ ด้วยเหตุนี้และเหตุอื่นๆ อีกหลายประการ แนวทางในการลงโทษของสหรัฐอเมริกาที่นำมาใช้กับอาชญากรรมคอมพิวเตอร์จึงเหมือนกับอาชญากรรมการฉ้อโกงทั่วๆ ไป ภายใต้แนวทางนี้ หลังจากที่ทำการประเมินระดับของการกระทำความผิดแล้ว ระยะเวลาในการลงโทษผู้กระทำผิดจะถูกกำหนดโดยการคำนวณทางคณิตศาสตร์ของการลงโทษที่ได้มีการกำหนดไว้แล้ว และหักปัจจัยที่ทำให้มีการลดโทษออก ซึ่งนำไปสู่การใช้ตารางการลงโทษ ซึ่งขึ้นอยู่กับประวัติอาชญากรรมเป็นตัวกำหนดแนวทางของระยะเวลาการลงโทษของการกระทำผิดนั้น แนวทางเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์นั้นผูกติดอยู่กับแนวทางการฉ้อโกงทั่วๆ ไป แนวโน้มการลงโทษจะขึ้นอยู่กับการคำนวณความเสียหายเป็นหลัก ซึ่งดูเหมือนจะเหมาะสม กล่าวคือผู้ที่ฉ้อโกงผู้อื่นมา 500 เหรียญย่อมจะมีโทษเบากว่าผู้ที่ฉ้อโกงผู้อื่นมา 5 ล้านเหรียญ แต่วิธีการเช่นนี้ดูจะไม่เหมาะสมกับอาชญากรรมคอมพิวเตอร์ ความสูญเสียที่เกิดขึ้นกับผู้ใช้คอมพิวเตอร์ในการบุกรุกแบบธรรมดา หรือการดูข้อมูลเฉยๆ นั้นเป็นเท่าใด มีการพิจารณามูลค่าของข้อมูลหรือไม่ จะคำนวณอย่างไร มีความแตกต่างหรือไม่ระหว่างการที่ข้อมูลนั้นได้ถูกนำไปใช้แล้วจริงๆ กับการที่มีเจตนาจะนำไปใช้แต่ยังไม่ได้ใช้ ควรจะมีการรวมค่าใช้จ่ายในการสืบสวน สอบสวน หรือการแก้ไขระบบรวมไว้ในความเสียหายที่เกิดขึ้นหรือไม่ การ

ลงโทษผู้กระทำผิดควรจะขึ้นอยู่กับความเสียหายที่เจตนาจะให้เกิด หรือความเสียหายที่เกิดขึ้นจริง การลงโทษผู้กระทำผิดควรจะขึ้นอยู่กับระดับของทักษะที่จะต้องใช้ในการกระทำผิดนั้น หรือตำแหน่งที่อำนวยความสะดวกในการเข้าถึงคอมพิวเตอร์ หรือจะขึ้นอยู่กับธรรมชาติของการกระทำผิดล้วนๆ แนวทางในการลงโทษนั้นได้รับการตราออกมาเพื่อทำให้เกิดการลงโทษที่เท่าเทียมกันและแน่นอน อย่างไรก็ตาม ในวิธีนี้การที่ไม่สามารถตอบคำถามเหล่านี้ได้ก็ยิ่งทำให้สิ่งต่างๆ ยุ่งยากขึ้น ความแตกต่างเหล่านี้ หมายถึง ความแตกต่างตั้งแต่การรอลงอาญาไปจนถึงการลงโทษจำคุกสำหรับผู้กระทำความผิดรุนแรง เนื่องจากจุดมุ่งหมายของกฎหมายอาชญากรรมนั้น คือ การยับยั้งและการลงโทษ ความไม่ชัดเจนของแนวทางการลงโทษทำให้ความศักดิ์สิทธิ์ของกฎหมายอาชญากรรมคอมพิวเตอร์และอาชญากรรมอื่นๆ นั้นลดลง ดังนั้น ในปี 1994 คณะกรรมาธิการพิจารณาโทษของสหรัฐอเมริกาซึ่งมีความรับผิดชอบในการร่างแนวทางในการลงโทษ รับทราบว่าอาชญากรรมคอมพิวเตอร์มักจะเกี่ยวข้องกับความเสียหายในเชิงเศรษฐกิจ อีกทั้งยังเกี่ยวข้องกับความเสียหายในเรื่องของความเป็นส่วนตัว และความปลอดภัยด้วย ทั้งความเสียหายที่เกิดจากค่าใช้จ่ายในการแก้ไขระบบ และความเสียหายที่เกิดขึ้นตามมา นอกจากนี้ เนื่องจากเทคโนโลยีคอมพิวเตอร์ถูกพัฒนาขึ้นอย่างรวดเร็วจนทำให้เห็นถึงความไม่เพียงพอของบทบัญญัติในกฎหมายฉบับนี้ ผู้เสียหายที่เป็นนิติบุคคลยังคงปิดบังการกระทำความผิดทางอาญาที่เกิดขึ้น และแม้จะมีการลงโทษ Hacker วัยรุ่นหลายรายแต่ก็ยังมีการวิจารณ์กันว่ากฎหมายยังมิได้กำหนดบทลงโทษอาชญากรมืออาชีพ เช่น พนักงานที่อยู่ภายในบริษัทซึ่งสามารถเป็นตัวทำลายและก่อให้เกิดความเสียหายได้มากกว่า ดังนั้น คณะกรรมการจึงเสนอแนวทางในการลงโทษใหม่ที่ใช้กับทั้งบุคคลและองค์กรในเรื่องของอาชญากรรมคอมพิวเตอร์ มีการเพิ่มโทษอย่างมากสำหรับการใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลที่เป็นความลับ ความผิดอาญาเกี่ยวกับการจงใจหลอกลวงผู้บริสุทธิ์เพื่อให้เกิดความเสียหาย การยึดอุปกรณ์คอมพิวเตอร์ที่ใช้ในการเข้าถึงโดยปราศจากอำนาจ การเพิ่มโทษต่อผู้ที่กระทำความผิดเป็นครั้งที่สอง แม้ว่าจะมิได้กระทำความผิดซ้ำในอนุมาตราเดียวกัน[24]

ต่อมาในเดือนมิถุนายน ปี 1996 ได้มีการศึกษาโดย The United States Sentencing Commission ได้ข้อสรุปว่ามีเพียง 174 คดีที่กฎหมายต่างๆ ซึ่งรวมถึงกฎหมายฉบับนี้นำมาใช้ในการลงโทษ และยอมรับว่าปัญหาต่างๆ ยังไม่ได้รับการแก้ไขเท่าที่ควร การกระทำผิดบางอย่างอันเกี่ยวกับคอมพิวเตอร์ยังถูกนำไปฟ้องร้องดำเนินคดีตามกฎหมายฉบับอื่นแตกแยกกันออกไป ดังนั้น จึงเห็นได้ว่าการจัดรวบรวมคดีอาชญากรรมคอมพิวเตอร์มาอยู่ในศูนย์กลางภายใต้กฎหมายฉบับเดียวน่าจะทำให้การวัดปริมาณความเสียหายที่มีอยู่ดีขึ้น สามารถคาดการณ์ถึงแนว

---

[24] Ibid.

โน้มและพิจารณาความจำเป็นในการปฏิรูปกฎหมายเพิ่มเติมได้ นอกจากนี้ การแก้ไขปรับปรุงแบบแผนการพิจารณาโทษจะมีประสิทธิผลมากขึ้น จึงได้มีการแก้ไขปรับปรุงกฎหมายอีกครั้งซึ่งบังคับใช้อยู่จนถึงปัจจุบัน

สาระสำคัญของกฎหมายมาตรา 1030 ฉบับปัจจุบัน (แก้ไขปี 1996) ในส่วนที่เกี่ยวข้องกับการปกป้องข้อมูลในระบบคอมพิวเตอร์ ได้แก่

มาตรา 1030 (a) (2) มาตรานี้ถูกบัญญัติขึ้นเพื่อป้องกันความลับของข้อมูลในคอมพิวเตอร์ คณะกรรมการ Senate Judiciary Committee ได้ตั้งข้อสังเกตเมื่อปี 1986 ว่าจุดมุ่งหมายสำคัญในมาตรานี้เป็นเรื่องการปกป้องข้อมูลซึ่งได้บันทึกไว้ในคอมพิวเตอร์และข้อมูลซึ่งเกี่ยวข้องกับความสัมพันธ์ของลูกค้ากับสถาบันการเงิน และเนื่องจากเหตุผลของอนุมาตรานี้เป็นเรื่องของการปกป้องข้อมูลส่วนบุคคล ดังนั้น คณะกรรมการดังกล่าวจึงมีความประสงค์ที่จะทำให้เกิดความกระจ่างว่า ข้อมูลในบริบทนี้จะเป็นเพียงข้อมูลที่มีการบันทึกไว้เท่านั้น อย่างไรก็ตาม ด้วยวิวัฒนาการซึ่งเป็นไปอย่างต่อเนื่อง สภาคองเกรซจึงให้การรับรองว่าข้อมูลด้านการเงินและด้านเครดิตจะต้องได้รับการปกป้องจากรัฐบาลกลาง ในหลักเกณฑ์ต่างๆ ของ NII (The National Information Infrastructure) จะสันนิษฐานไว้ก่อนว่า ข้อมูลที่มีความอ่อนไหวต่อการถูกลักขโมย (Sensitive Information) จะอยู่ในข่ายซึ่งสามารถถูกล้วงเอาโดยบุคคลภายนอกซึ่งมีเครือข่ายคอมพิวเตอร์ประสานกันเป็นจำนวนมาก ดังนั้น NII จะประสบผลสำเร็จอย่างดียิ่งในการดำเนินการ หากข้อมูลส่วนบุคคลได้รับการป้องกันอย่างเหมาะสม ด้วยเหตุนี้อนุมาตรานี้จึงได้บัญญัติขึ้นมาเพื่อประกันว่าการใช้คอมพิวเตอร์โดยมิชอบเพื่อให้ได้มาซึ่งข้อมูลของทางราชการหรือเพื่อให้ได้ไว้ในความครอบครองของเอกเชนจะต้องได้รับโทษ บทบัญญัติได้ถูกปรับปรุงแก้ไขให้มีการเพิ่มโทษหรือปรับเปลี่ยนโทษได้หากต้องการ อย่างไรก็ตาม มิอาจประกันได้ว่าการใช้คอมพิวเตอร์โดยมิชอบจะได้รับการลงโทษจากส่วนกลางเสียทั้งหมด ปัญหาสำคัญก็คือไม่สามารถแยกแยะข้อมูลที่สำคัญและไม่สำคัญออกจากกันได้อย่างชัดเจน ดังนั้น การกระทำเพื่อให้ได้มาซึ่งข้อมูลทุกประเภทจึงถือเป็นความผิดทางอาญา ซึ่งไม่เพียงแต่การเบียดบังเอาข้อมูลไปเท่านั้น การใช้วิธีการต่างๆ โดยทุจริต เช่น การมอบอำนาจให้บุคคลใดบุคคลหนึ่งใช้คอมพิวเตอร์ของผู้อื่นให้กระทำการ รวมทั้งการใช้อำนาจเกินขอบเขต (exceed of authority) เพื่อให้ได้มาซึ่งข้อมูลของผู้อื่นก็ถือเป็นความผิด

อนุมาตรา (a) (2) (C) บัญญัติขึ้นเพื่อป้องกันการโจรกรรมข้อมูลโดยใช้คอมพิวเตอร์ในต่างประเทศหรือระหว่างประเทศ บทบัญญัตินี้สืบเนื่องจากแนวทางในการ

พิจารณาคดีของ The Tenth Circuit's Decision ในคดีระหว่าง United States v. Brown คดีนี้ศาลพิจารณาว่าทรัพย์สินทางปัญญาอันเป็นนามธรรม (Intangible Intellectual Property) เช่น โปรแกรมคอมพิวเตอร์ ไม่สามารถทำหรือประกอบให้เป็นสินค้า ผลิตภัณฑ์ หลักทรัพย์ หรือเงินซึ่งถูกโจรกรรมและเปลี่ยนแปลงรูปโฉมหรือถูกนำไปตามความหมายของอนุมาตรา 2314 (18 U.S.C. sec 2134) แต่สำหรับอนุมาตรานี้ คำว่า "ข้อมูล" เป็นการตีความกว้างๆ และจะรวมไปถึงข้อมูลซึ่งถูกเก็บรักษาไว้ในรูปแบบที่ไม่สามารถสัมผัสได้ นอกจากนี้คำว่า "การรับข้อมูล" ซึ่งอยู่ในอนุมาตรา 1030(a) (2) จะครอบคลุมแม้จะกระทำโดยเพียงการอ่านข้อมูลก็ตาม ในแวดวงอิเล็คทรอนิคส์ ข้อมูลสามารถขโมยกันได้โดยที่ต้นฉบับมักจะไม่ถูกแตะต้อง

ความรุนแรงของการกระทำความผิดในส่วนที่เป็นการเบียดบังหรือลักลอบเอาข้อมูลไป จะขึ้นอยู่กับมูลค่าของข้อมูลหรือการให้เหตุผลของผู้กล่าวหา ด้วยเหตุนี้ โทษตามที่กำหนดไว้ในกฎหมายจึงจัดเป็นระดับ เช่น กรณีการรับหรือเบียดบังเอาข้อมูลเพียงเล็กน้อยก็ถือเป็นความผิดเล็กน้อย (Misdemeanor) แต่หากมีองค์ประกอบในการกระทำผิดหลายอย่างประกอบกันเข้า ก็อาจเป็นความผิดทางอาญาได้ ยิ่งกว่านั้นคดีจะเป็นอาชญากรรมร้ายแรงถ้าความผิดซึ่งกระทำขึ้นนั้น กระทำเพื่อวัตถุประสงค์ในการหาประโยชน์ทางการค้าหรือเพื่อให้ได้ประโยชน์ทางด้านการเงินเป็นการส่วนตัว หรือมีวัตถุประสงค์ที่จะกระทำผิดในทางอาญาหรือทางแพ่งอันเป็นการฝ่าฝืนรัฐธรรมนูญหรือกฎหมายของรัฐหรือรัฐบาลกลาง หรือข้อมูลที่เบียดบังมานั้นมีมูลค่าเกินกว่า 5,000 เหรียญสหรัฐ สำหรับด้านการเงินนั้น วิธีการบางอย่างสามารถนำมาเพื่อใช้สร้างมูลค่าของข้อมูลที่เบียดบังเอาไปได้ เช่น ต้นทุนในการผลิต พัฒนา วิจัย หรือมูลค่าของทรัพย์สินในตลาดของกลุ่มพวกขโมยข้อมูล (The Thieves Market) ซึ่งมีการสร้างมูลค่าตามที่กำหนดเท่ากับ 5,000 เหรียญสหรัฐได้

มาตรา 1030 (a) (3) จะป้องกันข้อมูลในระบบคอมพิวเตอร์จากบุคคลภายนอก แม้ว่าจะไม่ได้ข้อมูลไปก็ตาม และป้องกันบุคคลภายในซึ่งฝ่าฝืนจรรยาบรรณโดยใช้คอมพิวเตอร์หาข้อมูลในข่ายงานโดยมิชอบก็จะต้องรับผิด แม้ว่าจะไม่ทำให้ข้อมูลอันเป็นความลับเสียหายก็ตาม ส่วนอนุมาตรา 1030 (a) (2) จะบัญญัติไว้ในทางตรงกันข้าม คือ จะป้องกันข้อมูลที่เป็นความลับแม้กระทั่งกับบุคคลภายในที่มีเจตนาใช้คอมพิวเตอร์โดยทุจริต นอกจากนี้ แม้ว่าการฝ่าฝืนอนุมาตรา 1030 (a) (3) ในครั้งแรกจะเป็นเพียงความผิดเล็กน้อย แต่สำหรับอนุมาตรา 1030 (a) (2) จะบัญญัติให้การฝ่าฝืนเช่นว่านั้นเป็นอาชญากรรม ถ้าข้อมูลที่ได้รับไปนั้นเป็นข้อมูลที่มีค่าหรือนำไปใช้โดยทุจริตอย่างชัดเจน แม้ว่าการกระทำเพียงครั้งเดียวน่าจะเป็นความผิดเล็กน้อย แต่บท

บัญญัติดังกล่าวต้องการให้ความคุ้มครองมากขึ้นเนื่องจากการกระทำเช่นนั้นอาจทำให้เกิดความเสียหายในรูปแบบต่างๆ ตามมาได้

มาตรา 1030 (a) (4) ได้รับการแก้ไขเพิ่มเติมเพื่อประกันว่าบุคคลจะได้รับการลงโทษหากมีการกระทำผิดถึงขั้นเป็นอาชญากรรมโดยใช้คอมพิวเตอร์เพื่อให้ได้รับหรือเบียดบังเอาข้อมูลของผู้อื่นไปโดยปราศจากอำนาจ หรือแม้ว่าจะได้รับมอบอำนาจให้กระทำการเช่นนั้นแต่ได้ใช้อำนาจเกินขอบเขต เกี่ยวกับการใช้คอมพิวเตอร์นี้คณะกรรมการด้านการตุลาการของสภาซีเนทตั้งข้อสังเกตไว้ว่า การใช้หรือการบริการคอมพิวเตอร์จะมีคุณค่าในตัวของมันเอง ดังนั้น การลักลอบหรือเบียดบังเอาข้อมูลของผู้อื่นที่เก็บไว้ในระบบคอมพิวเตอร์ไปโดยทุจริตเป็นการทำให้ตัวจัดระบบข้อมูลในคอมพิวเตอร์เสียหายได้ ขณะเดียวกันคณะกรรมการดังกล่าวเห็นว่า ควรจะมีการแยกแยะให้เห็นชัดเจนระหว่างการกระทำที่เป็นการฉ้อโกง ภายใต้ข้อ (a) (4) ซึ่งจะต้องถูกลงโทษฐานกระทำการเป็นอาชญากร กับการกระทำในลักษณะที่เป็นการลักลอบหรือเบียดบังข้อมูลจะต้องถูกลงโทษฐานประพฤติมิชอบ

มาตรา 1030 (a) (5) อนุมาตรานี้เดิมเคยได้รับการปรับปรุงแก้ไขเมื่อปี 1994 โดยตัดคำว่า "Federal Interest Computer" ออกไป และนำคำว่า "Computer used in interstate commerce or communications" มาใช้แทน ซึ่งคำหลังนี้จะมีความหมายกว้างขวางมากกว่า เพราะความหมายของคำแรกนั้นจะครอบคลุมคอมพิวเตอร์ซึ่งเป็นหนึ่งในหลายคอมพิวเตอร์ที่ใช้ในการกระทำความผิด แต่ไม่ครอบคลุมถึงคอมพิวเตอร์ทุกๆ เครื่องในรัฐเดียวกัน นั่นหมายความว่า Hacker ที่โจรกรรมข้อมูลจากคอมพิวเตอร์เครื่องอื่นๆ ในรัฐเดียวก็ไม่อยู่ภายใต้เขตอำนาจของส่วนกลาง (Federal Jurisdiction) แม้ว่าการกระทำเช่นนั้นอาจจะส่งผลกระทบอย่างรุนแรงต่อการค้าระหว่างประเทศหรือระหว่างรัฐก็ตาม ดังนั้น จึงจำเป็นต้องมีการปรับปรุงแก้ไขกฎหมายในส่วนนี้ อย่างไรก็ตาม ภายหลังการแก้ไขแล้วก็ยังพบข้อบกพร่องบางประการ ดังนั้น ในปี 1996 จึงมีการแก้ไขโดยนำคำว่า "Protected Computer" มาใช้แทนคำทั้งสองข้างต้น ซึ่งถูกบัญญัติไว้ในอนุมาตรา 1030 (e) (2) โดยนำมาใช้ในอนุมาตรา 1030 (a) (5) อนุมาตรา 1030 (a) (2) อนุมาตรา 1030 (a) (4) และอนุมาตรา 1030 (a) (7) คำจำกัดความคำว่า "Protected Computer" จะมีความหมายครอบคลุมไปถึงคอมพิวเตอร์ของรัฐบาล สถาบันการเงิน และคอมพิวเตอร์ติดต่อระหว่างรัฐหรือระหว่างประเทศ คำจำกัดความซึ่งมีความหมายกว้างขวางเช่นนี้จะช่วยแก้ไขปัญหาการโจรกรรมข้อมูลคอมพิวเตอร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ด้วยเหตุที่เครือข่ายข้อมูลในโลกมีการขยายตัวอย่างต่อเนื่อง เป็นไปได้อย่างมากที่จะมีการโจรกรรมข้อมูลใน

โลกเพิ่มมากขึ้น จึงเป็นสิ่งจำเป็นที่สหรัฐจะมีเขตอำนาจเหนือคดีอาชญากรรมคอมพิวเตอร์ระหว่างประเทศ

ประเด็นสำคัญอีกประการหนึ่งในการปรับปรุงแก้ไขกฎหมายในปี 1996 เนื่องจากการแก้ไขกฎหมายอนุมาตรานี้ในปี 1986 กำหนดให้ผู้กระทำผิดซึ่งก่อให้เกิดความเสียหายเป็นบุคคลซึ่งไม่ได้รับมอบอำนาจ ดังนั้น เงื่อนไขนี้จึงไม่ใช้กับบุคคลภายใน แม้ว่าเขามีเจตนาที่จะรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการกระทำของเขาก็ตาม เนื่องจากกฎหมายเน้นที่อำนาจหน้าที่ของผู้เบียดบังข้อมูลในคอมพิวเตอร์แต่เพียงอย่างเดียว ต่อมาในปี 1994 จึงได้ตัดเอาข้อกำหนดอันเป็นการล่วงละเมิดออกไป ขณะเดียวกันได้กำหนดความผิดของผู้กระทำทั้งที่เป็นบุคคลภายนอกและภายใน แต่ก็ต้องการให้พิสูจน์ก่อนว่าบุคคลที่กระทำผิดนั้นได้ทำให้เกิดความเสียหายหรือไม่ ไม่ว่าจะโดยเจตนาหรือโดยประมาทก็ตาม กฎหมายในปี 1994 จะไม่ลงโทษบุคคลที่เบียดบังเอาข้อมูลใน "Federal Interest Computer" ตราบใดที่บุคคลนั้นไม่มีเจตนาที่จะก่อให้เกิดความเสียหาย กฎหมายในปี 1994 นี้เน้นในเรื่องเจตนาของผู้กระทำ ซึ่งก่อให้เกิดช่องว่างในการบังคับใช้กฎหมาย ดังนั้น ในปี 1996 จึงมีการแก้ไขกฎหมายโดยกำหนดให้บุคคลใดก็ตามซึ่งมีพฤติกรรมก่อให้เกิดความเสียหายต้องรับผิดชอบในการกระทำนั้น เพราะจะเป็นการดีหากอนุมาตรานี้บัญญัติให้ความเสียหายจากการใช้คอมพิวเตอร์ซึ่งเกิดจากบุคคลภายนอกเป็นความผิดทั้งหมด รวมทั้งความเสียหายที่เกิดจากเจตนาของบุคคลภายในก็ต้องถือเป็นความผิดทางอาญาด้วย โดยมีการจัดระดับโทษไว้ดังนี้

1. ความเสียหายอันเกิดจากเจตนาที่กระทำโดยบุคคลภายนอกซึ่งไม่มีอำนาจและการกระทำโดยเจตนาของบุคคลภายใน ถือเป็นความผิดอาญา
2. ความเสียหายอันเกิดจากความไม่เจตนาที่กระทำโดยบุคคลภายนอกซึ่งไม่มีอำนาจถือเป็นความผิดอาญา ส่วนที่กระทำโดยบุคคลภายในไม่ถือเป็นความผิด
3. ความเสียหายอันเกิดจากความประมาทที่กระทำโดยบุคคลภายนอกซึ่งไม่มีอำนาจถือเป็นการประพฤติผิด ส่วนที่กระทำโดยบุคคลภายในไม่ถือเป็นความผิด

นอกจากนี้ เพื่อให้สอดคล้องกับอนุมาตรา 1030 (a) (5) ที่ต้องการป้องกันสภาพความสมบูรณ์ในคอมพิวเตอร์ ป้องกันการลักลอบหรือเบียดบังเอาข้อมูลในคอมพิวเตอร์ จึงมีการบัญญัติคำว่า "ความเสียหาย" ให้มีความหมายกว้างยิ่งขึ้น และได้กำหนดคำใหม่ว่า "สิ่งที่เป็นภัย"

คือ สาเหตุที่ทำให้เกิดความเสียหายต่อร่างกาย ต่อบุคคล และการคุกคามต่อความปลอดภัยของสาธารณะ ด้วยเหตุที่คอมพิวเตอร์เปรียบเสมือนโครงสร้างของข่ายงานอื่นๆ ซึ่งเจริญเติบโตอย่างต่อเนื่อง และยังมีความสำคัญต่อระบบอื่นๆ ซึ่งอาจจะไม่สามารถคาดการณ์ได้ ด้วยเหตุนี้ จึงต้องมีคำจำกัดความคำว่า "ความเสียหาย" ให้ครอบคลุมความหมายของคำว่า "สิ่งที่เป็นภัย" ไว้ด้วย

มาตรา 1030 ที่ได้รับการแก้ไขครั้งสุดท้ายเมื่อปี 1996 ได้บัญญัติคำสำคัญลักษณะของการกระทำความผิด และบทกำหนดโทษไว้ดังนี้[25]

คอมพิวเตอร์ที่ได้รับการป้องกัน (Protected Computer) หมายถึง คอมพิวเตอร์ที่ถูกใช้โดยเฉพาะในสถาบันการเงิน หรือรัฐบาลสหรัฐอเมริกา หรือในกรณีที่คอมพิวเตอร์มิได้ถูกใช้โดยเฉพาะเพื่อการนั้น ได้ถูกใช้โดยหรือสำหรับสถาบันการเงิน หรือรัฐบาลสหรัฐอเมริกา และการกระทำจะถือว่าเป็นความผิดเมื่อเกิดผลกระทบต่อการใช้งานโดยหรือสำหรับสถาบันการเงินหรือรัฐบาล หรือที่ถูกใช้ในการค้าหรือการติดต่อสื่อสารระหว่างรัฐหรือต่างประเทศ

บันทึกทางการเงิน (Financial Record) หมายถึง ข้อมูลที่มาจากบันทึกใดๆ ที่ครอบครองโดยสถาบันการเงิน ที่เกี่ยวข้องกับความสัมพันธ์ระหว่างลูกค้ากับสถาบันการเงิน

การเข้าถึงเกินขอบอำนาจ (Exceeds Authorized Access) หมายถึง การเข้าถึงระบบคอมพิวเตอร์โดยมีอำนาจ แต่ได้ใช้การเข้าถึงนั้นเพื่อให้ได้ไป หรือเปลี่ยนแปลงข้อมูลในระบบคอมพิวเตอร์ โดยผู้เข้าถึงไม่มีสิทธิที่จะกระทำเช่นนั้น

ความเสียหาย (Damage) หมายถึง ความเสียหายต่อความสมบูรณ์ หรือการใช้งานของฐานข้อมูล โปรแกรม ระบบคอมพิวเตอร์ หรือข้อมูลซึ่ง

- สร้างความเสียหายเป็นมูลค่าไม่น้อยกว่า 5,000 เหรียญสหรัฐภายในระยะเวลา 1 ปี ต่อบุคคลใดบุคคลหนึ่งหรือมากกว่า
- แก้ไขหรือทำให้ศักยภาพในการทดสอบทางการแพทย์ การบำบัด หรือดูแลบุคคลใดบุคคลหนึ่งหรือมากกว่าลดน้อยลง
- สร้างความเสียหายทางกายภาพแก่บุคคลใดๆ หรือ
- คุมคามความปลอดภัยหรือสุขภาพของประชาชน

---

[25] 18 U.S.C. section 1030.

ลักษณะของการกระทำความผิดถูกบัญญัติไว้ ดังนี้[26]

ข้อ (a) ผู้ใด

(1) โดยรู้ดีเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินกว่าอำนาจในการเข้าถึง และโดยวิธีการของการกระทำเช่นนั้น ได้ไปซึ่งข้อมูลที่ได้ถูกกำหนดโดยรัฐบาลสหรัฐอเมริกาโดยคำสั่งฝ่ายบริหาร หรือบทบัญญัติแห่งกฎหมายที่ประสงค์จะคุ้มครองจากการเปิดเผยข้อมูลโดยปราศจากอำนาจเพื่อความจำเป็นในการป้องกันประเทศหรือความสัมพันธ์ต่างประเทศ หรือฐานข้อมูลที่ถูกควบคุมตามที่ได้ให้คำจำกัดความไว้ในวรรค y ของมาตรา 11 แห่งพระราชบัญญัติพลังงานปรมาณู ค.ศ.1954 โดยความจำเป็นที่อาจเชื่อได้ว่าข้อมูลที่ได้รับนั้นสามารถถูกใช้เป็นอันตรายต่อสหรัฐอเมริกา หรือเป็นประโยชน์แก่ต่างประเทศ อย่างจงใจ ติดต่อสื่อสาร ส่งมอบ ส่งผ่าน หรือเป็นเหตุให้ได้ติดต่อสื่อสาร ส่งมอบ หรือส่งผ่าน ข้อมูลข้างต้นแก่บุคคลใดที่ไม่มีสิทธิจะได้รับ หรือจงใจเก็บรักษาข้อมูลและมิได้ส่งมอบข้อมูลต่อเจ้าหน้าที่หรือลูกจ้างของสหรัฐอเมริกาซึ่งมีสิทธิจะได้รับ

(2) โดยเจตนาเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินกว่าอำนาจในการเข้าถึงและเนื่องด้วยการนั้นได้รับข้อมูลที่ถูกบรรจุอยู่ในบันทึกทางการเงินของสถาบันการเงิน หรือผู้ออกบัตรตามที่ได้ให้คำจำกัดความไว้ในมาตรา 1602 (n) ของบทที่ 15 หรือที่ถูกบรรจุอยู่ในแฟ้มของตัวแทนที่รายงานที่เกี่ยวกับการบริโภค ซึ่งคำเหล่านี้ได้ถูกจำกัดความไว้ในพระราชบัญญัติ Fair Credit Report (15 U.S.C.1681 et seq.)

   (A) ข้อมูลจากกรมหรือตัวแทนใดๆ ของสหรัฐอเมริกา หรือ

   (B) ข้อมูลจากคอมพิวเตอร์ที่ได้ถูกคุ้มครองแล้ว ถ้าหากการกระทำเกี่ยวข้องกับการติดต่อสื่อสารระหว่างรัฐหรือต่างประเทศ

(3) โดยเจตนาและโดยปราศจากอำนาจในการเข้าถึงระบบคอมพิวเตอร์ที่มิได้เปิดเผยต่อสาธารณะของกรมหรือตัวแทนของสหรัฐอเมริกา หรือเข้าถึงระบบคอมพิวเตอร์เช่นว่านั้นของกรมหรือตัวแทน ที่ถูกสงวนไว้เป็นการเฉพาะสำหรับการใช้โดยรัฐบาลแห่งสหรัฐอเมริกา หรือในกรณีที่คอมพิวเตอร์มิได้ถูก

---

[26] Ibid.

สงวนไว้เป็นการเฉพาะ แต่ได้ถูกใช้โดยหรือเพื่อรัฐบาลของสหรัฐอเมริกา และการกระทำนั้นกระทบต่อการใช้โดยหรือสำหรับรัฐบาลแห่งสหรัฐอเมริกา

(4) โดยรู้อยู่และโดยเจตนาที่จะฉ้อโกงเข้าถึงระบบคอมพิวเตอร์ที่ถูกป้องกันแล้ว โดยปราศจากอำนาจหรือเกินกว่าอำนาจในการเข้าถึง และโดยวิธีการเข้าถึงเช่นนั้นสืบเนื่องกับการฉ้อโกง ได้รับสิ่งมีค่าไป เว้นแต่วัตถุประสงค์ของการฉ้อโกงและสิ่งที่ได้รับไปเป็นแต่เพียงเพื่อการใช้คอมพิวเตอร์และมูลค่าของการใช้ไม่เกินกว่า 5,000 เหรียญสหรัฐในรอบระยะเวลา 1 ปี

(5)

(A) โดยรู้อยู่เป็นเหตุให้มีการส่งผ่านของโปรแกรมข้อมูล รหัส หรือคำสั่ง และโดยผลของการกระทำนั้น โดยเจตนาและปราศจากอำนาจ สร้างความเสียหายต่อคอมพิวเตอร์ที่ถูกป้องกันแล้ว

(B) โดยเจตนาและโดยปราศจากอำนาจเข้าถึงระบบคอมพิวเตอร์ที่ถูกป้องกันแล้ว และโดยผลของการกระทำนั้นโดยปราศจากความระมัดระวังได้สร้างความเสียหาย หรือ

(C) โดยเจตนาและปราศจากอำนาจเข้าถึงระบบคอมพิวเตอร์ที่ถูกป้องกันแล้ว และโดยผลของการกระทำนั้นสร้างความเสียหาย

(6) โดยรู้อยู่และโดยเจตนาฉ้อโกง ค้า (ดังที่ให้คำจำกัดความไว้ในมาตรา 1029) ด้วยรหัสผ่านใดๆ หรือข้อมูลที่คล้ายคลึงกันซึ่งใช้ในการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ ถ้า

(A) การค้านั้นกระทบต่อการค้าระหว่างรัฐหรือต่างประเทศ หรือ

(B) คอมพิวเตอร์นั้นถูกใช้โดยหรือเพื่อรัฐบาลของสหรัฐอเมริกา

(7)โดยเจตนาที่จะรีดเอาเงินหรือสิ่งมีค่าจากบุคคล บริษัท สมาคม สถาบันการศึกษา สถาบันการเงิน หน่วยงานรัฐบาล หรือนิติบุคคลอื่นใด ส่งไปในการค้าระหว่างรัฐหรือต่างประเทศ ซึ่งข้อมูลใดๆ ที่บรรจุคำที่จะสร้างความเสียหายต่อคอมพิวเตอร์ที่ถูกป้องกันแล้ว

กฎหมายฉบับนี้ได้กำหนดโทษไว้ในข้อ (c) ดังนี้

- ผู้กระทำหรือพยายามกระทำความผิดตามข้อ (a) (1) ต้องโทษปรับตามบทนี้หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ หากผู้กระทำผิดเคยรับโทษสำหรับความผิดในอนุมาตราอื่นของมาตรานี้มาแล้ว หรือพยายามกระทำความผิดในอนุมาตราอื่นและอาจถูกลงโทษ ต้องระวางโทษจำคุกไม่เกิน 20 ปี

- ความผิดตามข้อ (a) (2) (3) (5) (C) หรือ (6) ต้องโทษปรับตามบทนี้ หรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ ความผิดตามข้อ (a) (2) หากได้กระทำเพื่อวัตถุประสงค์สำหรับความได้เปรียบทางการค้า หรือประโยชน์ส่วนตัวทางการเงิน ถูกกระทำโดยสืบเนื่องจากการกระทำทางอาญาหรือละเมิดโดยฝ่าฝืนต่อรัฐธรรมนูญหรือกฎหมายของสหรัฐอเมริกาหรือรัฐใดๆ หรือมูลค่าของข้อมูลที่ได้ไปไม่เกิน 5,000 เหรียญสหรัฐ

- ความผิดตามข้อ (a) (4), (5) (A), (5) (B), หรือ (7) ต้องโทษปรับตามบทนี้ หรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ

- ความผิดตามข้อ (a) (2) (3) (4) (5) (A), (5) (B), (5) (C), (6) หรือ (7) หากผู้กระทำผิดเคยรับโทษสำหรับความผิดในอนุมาตราอื่นของมาตรานี้มาแล้ว หรือพยายามกระทำความผิดในอนุมาตราอื่นและอาจถูกลงโทษ ต้องระวางโทษจำคุกไม่เกิน 10 ปี

อาชญากรรมทางคอมพิวเตอร์เกิดขึ้นจากการกระทำและจุดประสงค์ที่แตกต่างกันหลากหลายรูปแบบ ความผิดบางอย่างผู้กระทำก่อให้เกิดขึ้นเพื่อประโยชน์ในการกระทำความผิดอื่นตามมา เช่น กรณีที่ผู้กระทำผิด hack เข้าไปในระบบคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งหมายเลขบัตรเครดิตหรือข้อมูลอื่น เป็นต้น การกระทำดังกล่าวถือเป็นความผิดตามกฎหมายนี้ ดังคดีที่ขึ้นสู่ศาลและได้รับการตัดสินไว้แล้วหลายคดี[27] ดังนี้

คดี Hack (December 1, 2000) ระหว่าง United States of America โจทก์ Raymond Torricelli จำเลย เป็นคดีที่จำเลยใช้โปรแกรมที่เรียกว่า "rootkit" ซึ่งเป็นโปรแกรมที่หากนำไปใช้ (run) บนเครื่องคอมพิวเตอร์ใดแล้ว จะทำให้สามารถใช้งานได้ทุกหน้าที่ (function) ของเครื่องนั้นโดยไม่ต้องได้รับอนุญาตก่อน ซึ่งจำเลยได้เจาะระบบคอมพิวเตอร์เข้าไปในคอมพิวเตอร์ของ NASA Jet Propulsion Lab และใช้โปรแกรมดังกล่าวทำให้สามารถใช้คอมพิวเตอร์จาก Lab ดังกล่าวในการเข้าสู่ห้องสนทนาในอินเตอร์เนท และได้ติดตั้งโปรแกรมเพื่อดักฟัง (intercept) ชื่อผู้ใช้ (usernames) และรหัสผ่าน (passwords) จากเครื่องที่เข้ามาสนทนาด้วยเพื่อนำไปใช้ในการเข้าอินเตอร์เนท รวมทั้งหมายเลขบัตรเครดิต นอกจากนั้นยังใช้คอมพิวเตอร์ในการเข้าไปเปลี่ยนแปลงผลรางวัล MTV Movie Awards ซึ่งศาล US District Court , District of New York ได้ตัดสินลงโทษจำคุกและปรับจำเลย

คดี Hack (September 21, 2000) ระหว่าง United States of America โจทก์

---

[27] ข้อมูลดังกล่าวแปลมาจาก Hacker ใน Http://www.usdoj.gov , (12 July 2001).

ไม่เปิดเผยชื่อ (juvenile) จำเลย เป็นคดีที่จำเลยซึ่งใช้ชื่อในอินเตอร์เนทว่า "comrade" ยอมรับว่าได้ทำการเจาะระบบเครือข่ายคอมพิวเตอร์ของ Defence Threat Reduction Agency (DTRA) โดยเป็นหน่วยงานหนึ่งในกระทรวงกลาโหมสหรัฐอเมริกา จำเลยรับสารภาพว่าได้เจาะระบบเข้าไปใน server ของหน่วยงานโดยไม่ได้รับอนุญาตและแอบติดตั้ง "backdoor" ไว้บน server ซึ่งโปรแกรมดังกล่าวทำให้สามารถดักฟังข้อความที่ส่งออกหรือเข้ามาของพนักงานในหน่วยงาน รวมทั้งสามารถดักฟังบัญชีรายชื่อผู้ใช้และรหัสผ่านคอมพิวเตอร์ของเจ้าหน้าที่ในหน่วยงาน นอกจากนี้จำเลยยังเจาะเข้าไปในคอมพิวเตอร์ของ NASA ที่มีมูลค่าถึง 1.7 ล้านเหรียญสหรัฐ โดยเป็นซอฟต์แวร์ที่ใช้ในการตรวจสภาพแวดล้อมซึ่งใช้ในสถานีอวกาศ จากการกระทำดังกล่าวทำให้ศาล US District Court in Miami ตัดสินให้กักขัง (detention facility) จำเลยเป็นเวลา 6 เดือน

คดี Hack (September 6, 2000) ระหว่าง United States of America โจทก์ Patrick W. Gregory จำเลย คดีนี้เป็นความผิดที่เกี่ยวเนื่องกับมาตรา 1029 (a) 2 (การกระทำผิดที่ผู้กระทำรู้อยู่และเจตนาที่จะฉ้อโกง ค้า หรือใช้ access device ที่ไม่ได้รับอนุญาตหนึ่งชิ้นขึ้นไปในรอบระยะเวลา 1 ปี และโดยการกระทำเช่นว่านั้นไปได้ไปซึ่งสิ่งมีค่ารวมกันเป็นจำนวน 1,000 เหรียญสหรัฐขึ้นไปในรอบระยะเวลานั้น) ข้อเท็จจริงในคดีนี้เป็นช่วงระหว่างปี 1997-1999 จำเลยกับพวกเป็นสมาชิกกลุ่มนักเจาะระบบที่ใช้ชื่อว่า "total-kaOs" และ "globalHell" ได้ร่วมกันเจาะระบบเพื่อขโมยอุปกรณ์การเข้าถึงโดยไม่ได้รับอนุญาต (unauthorised access device) ได้แก่ หมายเลขโทรศัพท์, หมายเลขประจำตัว (PIN) และหมายเลขบัตรเครดิต รวมทั้งนำอุปกรณ์ที่ขโมยมาติดตั้งการบริการประชุมโทรภาพทางไกล (teleconference) ในหมู่สมาชิกโดยไม่ได้รับอนุญาต นอกจากนั้นยังแอบฟังหรือรบกวนการประชุมทางไกลของบุคคลอื่น รวมทั้งทำลายข้อมูลต่างๆ ภายหลังจากที่ได้เจาะระบบคอมพิวเตอร์ของเจ้าของ จากการกระทำดังกล่าวจำเลยถูกศาล US District Court , Northern District of Texas ตัดสินให้จำคุก 26 เดือน คุมความประพฤติ 3 ปีภายหลังพ้นโทษ และให้ชดใช้ค่าเสียหายจำนวน 154,529.86 เหรียญสหรัฐ

ในเรื่องเขตอำนาจศาลนั้น มีการระบุแนวทางในการวินิจฉัยข้อพิพาทเกี่ยวกับคดีอินเตอร์เนทที่น่าสนใจ คือ คดีระหว่าง Zippo Manufacturing Company และ Zippo.com,Inc. ซึ่งศาลได้วางแนวทางในเรื่องเขตอำนาจศาลไว้ว่า การที่ศาลจะพิจารณาและมีอำนาจเหนือจำเลยซึ่งอยู่ต่างประเทศนั้น จะต้องมีจุดคาบเกี่ยวเกิดขึ้น ซึ่งอาจพิจารณาได้จากปัจจัยต่อไปนี้[28]

---

[28] ไพบูลย์ อมรภิญโญเกียรติ, ร่างกฎหมายอาชญากรรมทางคอมพ์กับปัญหาในทางปฏิบัติ , Http://www. bangkokbiznews.com, (3 November 2000).

1. เจตนาของจำเลยในการกระทำความผิด
2. ภาระของจำเลยในการสู้คดีในศาล
3. ข้อขัดแย้งระหว่างอำนาจอธิปไตยของจำเลยและโจทก์
4. ผลประโยชน์ของรัฐที่ได้จากการตัดสินคดี
5. ทางแก้ไขข้อพิพาทที่มีประสิทธิภาพมากที่สุด
6. ผลประโยชน์ของโจทก์และมาตรการเยียวยาความเสียหายของโจทก์
7. ทางเลือกของการฟ้องคดีในศาลอื่น

หน่วยงานเฉพาะที่เกี่ยวข้องกับการทุจริตต่อบัตรเครดิตบนอินเตอร์เนท

United State Secret Service (U.S.S.S.)[29]

United State Secret Service (U.S.S.S.) เป็นหน่วยงานลับซึ่งมีหน้าที่สืบสวนคดีอาชญากรรมทางด้านการเงิน (Financial Crime) ขอบเขตอำนาจของหน่วยงานดังกล่าวรวมถึงสืบสวนคดีฉ้อโกงธนาคาร, การฉ้อโกง access device (รวมถึงบัตรเครดิต), อาชญากรรมทางด้านการสื่อสารและคอมพิวเตอร์, การทุจริตต่อข้อมูลส่วนบุคคล, การทุจริตต่อระบบรักษาความปลอดภัยของรัฐและการพาณิชย์ และการทุจริตต่อการโอนเงินทางอิเล็คทรอนิคส์

อำนาจหน้าที่ของ U.S.S.S. กับคดีทุจริตต่อบัตรเครดิตบนอินเตอร์เนท มีดังนี้

<u>การฉ้อโกง Access Device</u> (Access Device Fraud)

แหล่งข่าวทางด้านการเงินได้ประมาณการความสูญเสียที่เกิดขึ้นจากการทุจริตต่อบัตรเครดิตในแต่ละปีว่ามีมูลค่าสูงถึง 1,000 ล้านเหรียญสหรัฐ U.S.S.S. เป็นหน่วยงานเบื้องต้นที่มีหน้าที่สืบสวนคดีทุจริตต่อ Access Device หรือคดีอื่นๆ ที่เกี่ยวข้องภายใต้บทที่ 18 U.S.C. sec 1029 แม้ว่ากฎหมายฉบับนี้จะเป็นที่รู้จักกันในส่วนที่เกี่ยวข้องกับบัตรเครดิตเป็นส่วนมาก แต่ในความเป็นจริงแล้วกฎหมายดังกล่าวนำไปปรับใช้กับอาชญากรรมรูปแบบอื่นที่เกี่ยวข้องกับ Access Device เช่น เดบิตการ์ด, บัตรเอทีเอ็ม, รหัสคอมพิวเตอร์ (password) และ PINS (Personal Identification Numbers) เป็นต้น

---

[29] ข้อมูลดังกล่าวแปลมาจาก U.S.S.S.Financial Crime Division ใน Http://www.treas.gov/ usss/financial_crimes. htm, (12 July 2001).

การปลอมแปลงและทุจริตต่อข้อมูลส่วนบุคคล (Counterfeit and Fraudulent Identification)

ภายใต้บทที่ 18 U.S.C. sec 1028 ได้กำหนดให้การขโมยข้อมูลส่วนบุคคลเป็น Federal Crime และให้อำนาจแก่ U.S.S.S. รวมทั้ง FBI (Federal Bureau of Investigation) และหน่วยงานอื่นที่เกี่ยวข้องเป็นผู้มีอำนาจสืบสวนดำเนินคดีกับอาชญากรรมประเภทนี้

การฉ้อโกงทางคอมพิวเตอร์ (Computer Fraud)

ภายใต้บทที่ 18 U.S.C. sec 1030 ได้กำหนดให้ U.S.S.S. มีอำนาจสืบสวนคดีที่เทคโนโลยีและคอมพิวเตอร์ถูกนำมาใช้ในการกระทำความผิด คอมพิวเตอร์กำลังถูกใช้เป็นเครื่องมือประกอบอาชญากรรมทางการเงินอย่างแพร่หลาย ไม่เพียงใช้เป็นเครื่องมือประกอบอาชญากรรมโดยตรงเท่านั้น ยังใช้เพื่อการเจาะระบบเข้าสู่ฐานข้อมูลของผู้อื่นเพื่อการเปลี่ยนแปลงแก้ไขหรือลักลอบนำข้อมูลเหล่านั้นมาเพื่อใช้แสวงหาประโยชน์โดยมิชอบต่อไป

ด้วยเหตุที่คอมพิวเตอร์เป็นแหล่งข้อมูลขนาดใหญ่เพื่อนำไปสู่การสืบสวนและค้นหาพยานหลักฐาน ดังนั้น U.S.S.S. จึงจัดตั้งหน่วยงาน The Electronic Crimes Special Agent Program (ECSAP) เป็นตัวแทนที่มีบุคลากรที่ถูกฝึกสอนมาโดยเฉพาะเพื่อการควบคุม ดูแลรักษาและตรวจสอบระบบคอมพิวเตอร์ที่ถูกใช้ในการกระทำความผิด ให้คงอยู่ในสภาพเดิมที่สามารถใช้ประโยชน์เพื่อการสืบสวนและใช้เป็นพยานหลักฐานในการดำเนินคดีต่อไปได้

นอกจากนี้ U.S.S.S. มีอำนาจหน้าที่เกี่ยวพันร่วมกับหน่วยงานอื่นที่บังคับใช้กฎหมาย เช่น หน่วยงานของสหพันธรัฐ, รัฐ, เมือง และท้องถิ่น ทั้งนี้เพื่อเป้าหมายในการปราบปรามองค์กรอาชญากรรมระหว่างประเทศ และอาชญากรรมรูปแบบใหม่ๆ ที่เกิดขึ้น โดยทรัพย์สินทั้งหมดที่ยึดและริบได้จากการกระทำความผิด จะถูกจัดสรรให้แก่หน่วยงานต่างๆ ที่เกี่ยวข้อง เพื่อการพัฒนาบุคลากรและจัดหาวัสดุอุปกรณ์ที่ทันสมัย เพื่อใช้ในการสืบสวนและบังคับใช้กฎหมายอย่างมีประสิทธิภาพต่อไป เนื่องจากคอมพิวเตอร์และอุปกรณ์อิเล็คทรอนิคส์อื่นที่ทันสมัยได้ถูกนำมาใช้ในการประกอบอาชญากรรมอย่างแพร่หลาย ดังนั้น เจ้าหน้าที่ที่เกี่ยวข้องจึงควรต้องมีทักษะความรู้รวมถึงอุปกรณ์ที่ทันสมัยเทียบเท่ากับอาชญากรให้ได้

Federal Trade Commission (FTC)

FTC เป็นหน่วยงานกลางของรัฐบาลสหรัฐ เป็นหน่วยงานเบื้องต้นที่ให้การคุ้มครองผู้บริโภค มีเขตอำนาจครอบคลุมถึงเรื่องที่เกี่ยวข้องกับระบบเศรษฐกิจทั้งหมด รวมถึงการทำธุรกรรมของธุรกิจและผู้บริโภคบนอินเตอร์เนทด้วย ภายใต้ Federal Trade Commission Act ได้กำหนดให้ FTC มีอำนาจดำเนินการตอบโต้กับการกระทำที่ไม่ยุติธรรมหรือการหลอกลวง ทั้งนี้ เพื่อให้การแข่งขันทางด้านการตลาดเป็นไปอย่างสมบูรณ์

FTC มีอำนาจดำเนินคดีทางแพ่งต่อศาล เพื่อระงับการกระทำอันเป็นการหลอกลวงและเป็นการผิดต่อกฎหมายทั้งในระยะสั้นและระยะยาว เพื่อให้ผู้บริโภคที่ได้รับความเสียหายได้รับการชดใช้เยียวยา สิ่งเหล่านี้เป็นเครื่องมือในการต่อสู้กับการฉ้อโกงในรูปแบบต่างๆ ได้อย่างกว้างขวาง ซึ่งรวมถึงการฉ้อโกงที่เกิดขึ้นบนอินเตอร์เนทด้วย นอกจากนี้ FTC ยังมีอำนาจตามกฎหมายในเรื่องของ Identity Theft โดยเฉพาะ ตามที่บัญญัติไว้ใน Identity Theft and Assumption Deterrence Act of 1998 บทที่ 18 U.S.C. sec 1028 โดยเป็นหน่วยงาน (Clearing House) รับเรื่องราวร้องทุกข์และให้ความช่วยเหลือผู้ซึ่งตกเป็นเหยื่อ แม้ FTC จะไม่มีอำนาจนำเรื่องที่เกิดขึ้นไปสู่การดำเนินคดีทางอาญา แต่ก็สามารถจัดหาข้อมูลต่างๆ เพื่อช่วยเหลือและแก้ไขปัญหาให้แก่ผู้ที่ตกเป็นเหยื่อ ไม่ว่าจะเป็นปัญหาทางด้านการเงินหรือปัญหาอื่นใดก็ตามซึ่งเป็นผลจากอาชญากรรมนี้ โดย FTC จะเก็บรักษาข้อมูลของเหยื่อให้เป็นความลับ แต่ FTC อาจจัดส่งข้อมูลของเหยื่อไปยังหน่วยงานของรัฐหรือเอกชนที่เกี่ยวข้องเมื่อได้รับความยินยอมจากเหยื่อ ทั้งนี้เพื่อจัดหาหน่วยงานหรือองค์กรที่เหมาะสมให้เข้ามาดำเนินการให้เกิดผลคืบหน้ามากยิ่งขึ้นต่อไป ทั้งยังมีอำนาจทำการแก้ไขบันทึกทางด้านเครดิตของเหยื่อให้ถูกต้อง เนื่องจากเหยื่ออาชญากรรมประเภทนี้มักจะถูกรายงานทางเครดิตในด้านลบจากสถาบันการเงินหรือสถาบันผู้ออกบัตรเครดิตที่เกี่ยวข้อง[30]

4. The Electronic Communication Privacy Act of 1986

สิ่งสำคัญประการหนึ่งที่ควรต้องพิจารณาในการใช้เครือข่ายอินเตอร์เนท คือ สิทธิในความเป็นส่วนตัว (Right to privacy) ด้วยเหตุที่การใช้เครือข่ายอินเตอร์เนทจะได้รับประโยชน์สูงสุดเมื่อมีผู้ใช้บริการจำนวนมาก (Network Effect) และผู้ใช้มั่นใจว่าการใช้เครือข่ายส่ง

---

[30] ข้อมูลดังกล่าวแปลมาจาก Federal Trade Commission ใน Http://www.ftc.gov, (20 May 2001).

ผ่านข้อมูลนั้นจะได้รับความคุ้มครองจากการลักลอบหรือนำเอาข้อมูลไปใช้โดยบุคคลที่สามโดยไม่ได้รับอนุญาต ดังนั้น กฎหมายที่เกี่ยวกับการสื่อสารทางอิเล็คทรอนิคส์จึงควรจะให้ความคุ้มครองหรือรับรองสิทธิของผู้ใช้ในอันที่จะมีหรือใช้ระบบรักษาความปลอดภัย

สหรัฐอเมริกาเป็นประเทศหนึ่งที่ถูกจับตามองจากหลายประเทศถึงแนวโน้มการกำกับดูแลเครือข่ายอินเตอร์เนท เนื่องจากสหรัฐอเมริกามีการออกกฎหมายที่ใช้ในการกำกับดูแลการติดต่อสื่อสารผ่านเครือข่าย คือ The Electronic Communication Privacy Act of 1986 หรือ ECPA กฎหมายว่าด้วยการคุ้มครองความเป็นส่วนตัวในการสื่อสารทางอิเล็คทรอนิคส์ กฎหมายฉบับนี้เป็นกฎหมายแม่บทสำหรับการคุ้มครองการสื่อสารทางอิเล็คทรอนิคส์ และไม่ได้นำมาใช้เฉพาะกับบริการอินเตอร์เนทเท่านั้น แต่เป็นกฎหมายที่มีส่วนสำคัญยิ่งในการทำให้เครือข่ายอินเตอร์เนทเจริญเติบโตในประเทศสหรัฐอเมริกา[31]

ECPA ได้ถูกนำมาใช้เพื่อจัดการกับปัญหาสิทธิในความเป็นส่วนตัวตามกฎหมายและเพื่อขยายการคุ้มครองถึงการติดต่อสื่อสารบนสื่ออิเล็คทรอนิคส์รูปแบบใหม่ๆ ที่เกิดขึ้น ซึ่งรวมถึงเครื่องมือส่งข้อความทางวิทยุ (Radio paging device), ไปรษณีย์อิเล็คทรอนิคส์ (Electronic Mail), โทรศัพท์มือถือ (Cellular telephone), การส่งข้อความสื่อสารส่วนตัว (Private communication carriers) และการติดต่อทางคอมพิวเตอร์ (Computer transmissions)[32]

กฎหมายฉบับนี้ถูกพัฒนาขึ้นด้วยความคาดหวังให้สามารถจัดการกับปัญหาสิทธิในความเป็นส่วนตัว โดยกำหนดให้มีการควบคุมหน่วยงานและเจ้าหน้าที่ของรัฐ เช่น ตำรวจ สำนักข่าวกรอง สภาความมั่นคง ฯลฯ และควบคุมบุคคลทั่วไปมิให้กระทำผิดกฎหมายโดยการลักลอบดักฟังข้อมูลของผู้อื่นที่ปรากฏหรือถูกจัดเก็บอยู่ในสื่ออิเล็คทรอนิคส์ต่างๆ ทั้งนี้ เนื่องจากแต่เดิมนั้นกฎหมายคุ้มครองสิทธิส่วนบุคคลเกี่ยวกับการติดต่อสื่อสารนั้น มีเพียง The Wiretap Act ซึ่งให้ความคุ้มครองสำหรับการติดต่อสื่อสารทางสาย (Wire Communication) เท่านั้น โดยจำกัดเพียงการได้มาซึ่ง "เสียง" ในคดีระหว่าง United State v. Seidlitz ศาลได้ตัดสินว่าการดักฟังหรือรบกวน (Intercept) การติดต่อทางคอมพิวเตอร์ไม่ใช่การได้มาซึ่งเสียงจึงไม่อยู่ในความคุ้มครองของ The

---

[31] ดร.เลอสรร ธนสุกาญจน์ ผศ.ดร.จิตตภัทร เครือวรรณ์ ผศ.สุธรรม อยู่ในธรรม , <u>กฎหมายสำหรับบริการอินเตอร์เนทในประเทศไทย</u> , (กรุงเทพฯ : สำนักพิมพ์นิติธรรม , 2540) , หน้า 147.

[32] ข้อมูลดังกล่าวแปลมาจาก The Electronic Communication Privacy Act ใน Http://www.digitalcentury.com/ encyclo/update/ecpa. html, (7 May 2001).

Wiretap Act เพราะกฎหมายฉบับนี้ไม่คุ้มครองถึงข้อมูลที่ถูกจัดเก็บไว้ในระบบคอมพิวเตอร์ กฎหมายฉบับนี้จึงถูกมองว่ามิได้ให้ความคุ้มครองอย่างเพียงพอต่อการติดต่อสื่อสารและสิทธิในความเป็นส่วนตัว เนื่องจากให้ความคุ้มครองเฉพาะการติดต่อสื่อสารที่กระทำผ่านเทคโนโลยีบางอย่างเท่านั้น จึงจำเป็นต้องมีการพัฒนากฎหมายให้ขยายความคุ้มครองสิทธิในความเป็นส่วนตัวสำหรับการติดต่อสื่อสารทางสื่ออิเล็ก ทรอนิกส์สมัยใหม่ ทำให้เกิดเป็นกฎหมาย The Electronic Communication Privacy Act of 1986 หรือ ECPA[33]

ECPA ได้กำหนดให้การลักลอบดักฟังหรือรบกวนการสื่อสารระหว่างบุคคลทางสื่ออิเล็คทรอนิคส์เป็นการกระทำที่มิชอบด้วยกฎหมายและมีโทษทางอาญา โดยกำหนดว่า "ผู้ใดโดยเจตนา พยายาม หรือจัดการให้ผู้อื่น กระทำการดักฟังหรือรบกวนขัดขวางการติดต่อทางสายทางเสียง หรือทางสื่ออิเล็คทรอนิคส์ ต้องระวางโทษปรับหรือจำคุก"

กฎหมายฉบับนี้มีบทบัญญัติที่นำมาใช้กับผู้ให้บริการเครือข่าย (System Operator) โดยกฎหมายกำหนดห้ามมิให้บุคคลใดเข้าไปใช้เครือข่ายคอมพิวเตอร์[34] และมีบทบัญญัติที่ยกเว้นความผิดของผู้ให้บริการเครือข่ายไว้ในกรณีที่ตนจำเป็นต้องเห็น ดู หรืออ่านข้อความทางอิเล็กทรอ นิกส์ที่ส่งผ่านระหว่างบุคคลต่างๆ เพื่อสอดส่องดูแลความเรียบร้อยและสภาพการปฏิบัติงานของระบบ หากเป็นการดำเนินการโดยสุ่มตัวอย่างไม่เฉพาะเจาะจงการสื่อสารของบุคคลใดบุคคลหนึ่ง (random) และเป็นการกระทำตามปกติในทางการค้า หรือเพื่อปกป้องสิทธิหรือทรัพย์สินใดๆ ของผู้ให้บริการ[35] เช่น ผู้ให้บริการมีสัญญาอยู่กับผู้รับบริการว่าหากมีข้อร้องเรียนเกี่ยวกับการกระทำผิดกฎหมายของผู้ใช้บริการ ผู้ให้บริการสงวนสิทธิที่จะตรวจดูข้อความและถอนข้อความนั้นๆ ได้ เป็นต้น

นอกจากนี้ยังห้ามมิให้เปิดเผยหรือใช้โดยเจตนาซึ่งเนื้อหาของการติดต่อสื่อสารทางเสียง ทางสาย หรือทางสื่ออิเล็คทรอนิคส์ ซึ่งรู้หรือมีเหตุอันควรจะรู้ว่าได้รับมาจากการลักลอบ

---

[33] ข้อมูลดังกล่าวแปลมาจาก E-Law 2.0: Computer Information Systems Law and System Operator Liability Revisited ใน Http://www.austlii.edu.au/au/other/elaw/v1n03/loudy6.html, (3 November 2000).

[34] The Electronic Communication Privacy Act of 1986, 18 U.S.C. section 2701.

[35] Ibid, section 2511.

ดักฟังหรือรบกวนการสื่อสารอันเป็นการละเมิดต่อกฎหมายนี้[36] และห้ามผู้ให้บริการเครือข่ายเปิดเผยข้อความที่ตนได้มาแก่ผู้อื่นนอกเหนือไปจากบุคคลที่เป็นผู้รับตามคำสั่งที่มาทางอิเล็คทรอนิคส์นั้นๆ ดังนั้น ภาระหน้าที่ของผู้ให้บริการเครือข่ายจึงเกิดโดยกฎหมายในอันที่จะต้องรักษาความลับของผู้ใช้เครือข่ายของตน ซึ่งไม่จำกัดเฉพาะลูกค้าของตนเท่านั้น แต่ต้องรักษาความลับของบุคคลที่สามทุกคนที่ผ่านหรือสื่อสารเข้ามาในเครือข่ายของตน กฎหมายฉบับนี้แก้ไขในปี ค.ศ.1994 โดยกำหนดหน้าที่อย่างกว้างขวางสำหรับผู้ให้บริการเครือข่าย เนื่องจากเทคโนโลยีอินเตอร์เนทได้พัฒนาไปล้ำกว่าหลักกฎหมาย เพราะแต่เดิมนั้นกฎหมายให้ความคุ้มครองเฉพาะผู้ใช้เครือข่ายที่เป็นลูกค้าหรือผู้ที่ได้รับอนุญาตเท่านั้น แต่เมื่อเทคโนโลยีเครือข่ายพัฒนามาใช้เครือข่ายสาธารณะซึ่งไม่จำกัดเส้นทางและไม่จำกัดผู้ใช้ ดังนั้น กฎหมายจึงต้องขยายภาระหน้าที่ของผู้ให้บริการเครือข่ายว่าต้องรักษาความลับของทุกคนที่ผ่านเข้ามาในระบบของตน แม้ว่าจะไม่มีสัญญาผูกพันที่จะรักษาความลับแก่บุคคลนั้นก็ตาม

กฎหมายฉบับนี้มีข้อยกเว้นสำคัญประการหนึ่ง คือ ยอมให้รัฐบาลสามารถดักฟังหรือตรวจสอบข้อมูลการติดต่อทางอิเล็คทรอนิคส์ได้ โดยมาตรา 2511 (2) (a) (II) อนุญาตให้ผู้ให้บริการสื่อสารทางอิเล็คทรอนิคส์อนุญาตให้เจ้าหน้าที่ของรัฐที่มีอำนาจสามารถติดเครื่องมือดักฟังได้อย่างถูกต้องตามกฎหมาย หากได้ปฏิบัติตามเงื่อนไขที่กำหนดไว้ กล่าวคือ ได้รับคำสั่งศาลตามคำร้องขอของบุคคลที่กำหนดในกฎหมาย เช่น อัยการ รองอัยการ เพื่อให้พนักงานสอบสวนหรือ FBI สามารถดักฟังและอัดเทปข้อความที่ดักฟังได้ แต่มีข้อกำหนดว่าคดีหรือความผิดที่กำลังสอบสวนนั้นต้องเป็นความผิดร้ายแรงตามที่กฎหมายกำหนด เช่น จารกรรม กบฏ ปล้น ฟอกเงิน เป็นต้น ซึ่งในส่วนนี้รัฐต้องพิสูจน์ ดังนี้[37]

1. มีเหตุน่าเชื่อว่ามีการทำผิดกฎหมายเกิดขึ้นหรือกำลังจะเกิด
2. มีเหตุอันควรเชื่อได้ว่า การสื่อสารจะสามารถหาหรือนำมาได้โดยการดักฟังหรือลักลอบดักฟังการสื่อสาร
3. รัฐได้พยายามสืบสวนสอบสวนโดยวิธีอื่นตามปกติมาก่อนแล้ว แต่ไม่ได้ผลหรือเป็นไปได้ยากมากที่จะสำเร็จ
4. มีเหตุเชื่อได้ว่าสถานที่ที่จะใช้ในการดักฟังหรือลักลอบดักฟังการสื่อสารเป็นสถานที่ที่ใช้ประกอบอาชญากรรมหรือการติดต่อดังกล่าว

---

[36] Ibid, section 2511 (amended 1994).

[37] Ibid, section 2515.

สิทธิในความเป็นส่วนตัวในสถานที่ทำงานได้รับความคุ้มครองตามกฎหมายนี้ด้วย โดยนายจ้างไม่อาจบันทึกหรือดูการสนทนาทางโทรศัพท์หรือไปรษณีย์อิเล็คทรอนิคส์ (E-Mail) ของลูกจ้าง แต่มีข้อยกเว้นให้นายจ้างทำได้หากลูกจ้างได้รับการแจ้งเตือนล่วงหน้าหรือนายจ้างมีเหตุผลที่จะเชื่อว่าผลประโยชน์ของบริษัทกำลังตกอยู่ในอันตราย ในทศวรรษ 1990 มีคดีเกิดขึ้นหลายคดีที่ลูกจ้างฟ้องว่าสิทธิในความเป็นส่วนตัวของพวกเขากำลังถูกละเมิด และการควบคุมของบริษัทเกินขอบเขต ดังนั้น ในปี 1992 จึงมีการปรับปรุงแก้ไขกฎหมายในส่วนนี้ โดยกำหนดหลักเกณฑ์ดังนี้[38]

1. บังคับนายจ้างให้เปิดเผยข้อมูลเกี่ยวกับระบบการสอดส่องตรวจดูที่กระทำต่อลูกจ้าง และให้มีสัญญาณเตือนเมื่อการติดต่อสื่อสารกำลังถูกสอดส่อง
2. การสอดส่องทั้งหมดต้องเกี่ยวข้องกับงานที่จ้างเท่านั้น
3. จัดให้ลูกจ้างเข้าถึงข้อมูลที่เกี่ยวกับงานที่ได้รับผ่านการสอดส่อง
4. จำกัดการเปิดเผยและใช้ฐานข้อมูล

5. Fair Credit Billing Act[39]

Fair Credit Billing Act (FCBA) เป็นกฎหมายที่บัญญัติถึงขั้นตอนการแจ้งข้อร้องเรียนเกี่ยวกับการเรียกเก็บเงินค่าใช้จ่ายจากการใช้บัตรเครดิตที่มีข้อผิดพลาด (Billing Error) และกำหนดให้เจ้าหนี้ (ผู้ออกบัตร) ซึ่งอาจเป็นธนาคารหรือสถาบันการเงิน ให้ดำเนินการตรวจสอบและแจ้งผลไปยังผู้ถือบัตรตามที่ได้ร้องเรียนเข้ามา ไม่ว่าจะเป็นไปในทางยอมรับหรือปฏิเสธก็ตาม กฎหมายฉบับนี้เป็นส่วนหนึ่งของ Truth in Lending Act (TILA)

<u>การเรียกเก็บเงินที่มีข้อผิดพลาด</u> (Billing Error) รวมถึง

1. ใบเรียกเก็บเงินสำหรับธุรกรรมที่ไม่เคยเกิดขึ้น
2. การทำธุรกรรมโดยบุคคลผู้ปราศจากอำนาจ
3. ใบเรียกเก็บเงินที่มีการแจ้งจำนวนเงินผิดพลาด

---

[38] E-Law 2.0: Computer Information Systems Law and System Operator Liability Revisited.

[39] 15 U.S.C.sec.1666.

4. ใบเรียกเก็บเงินค่าสินค้าและบริการที่ยังไม่ถูกส่งถึงลูกค้า หรือยังไม่ได้รับการยอมรับจากลูกค้า
5. ความผิดพลาดจากระบบคอมพิวเตอร์

ขั้นตอนการแก้ปัญหาการเรียกเก็บเงินที่มีข้อผิดพลาด

1. ผู้ถือบัตรต้องแจ้งข้อร้องเรียนเป็นลายลักษณ์อักษร กล่าวคือ ต้องมีหนังสือบอกกล่าวแจ้งถึงการเรียกเก็บเงินที่มีข้อผิดพลาดไปยังเจ้าหนี้ภายในกำหนด 60 วัน นับแต่วันที่เจ้าหนี้ได้จัดส่งใบเรียกเก็บเงินฉบับแรกที่ปรากฏข้อผิดพลาดให้แก่ผู้ถือบัตร การจัดส่งหนังสือร้องเรียนนี้ ผู้ถือบัตรต้องส่งไปยังที่อยู่ของเจ้าหนี้ที่ระบุไว้เป็นการเฉพาะ ซึ่งอาจมิใช่ที่อยู่สำหรับการชำระเงิน หากเกิดกรณีที่คนร้ายแจ้งเปลี่ยนที่อยู่ในการจัดส่งใบเรียกเก็บเงินของผู้ถือบัตรไปยังที่อยู่แห่งใหม่ซึ่งมีผลทำให้ผู้ถือบัตรไม่ได้รับใบเรียกเก็บเงินนั้น ผู้ถือบัตรก็ยังคงมีหน้าที่ต้องจัดส่งหนังสือร้องเรียนไปยังเจ้าหนี้ภายในกำหนดเวลาข้างต้น และไม่อาจยกเหตุที่ตนไม่ได้รับใบเรียกเก็บเงินขึ้นเป็นข้อต่อสู้ได้ นั่นคือเหตุผลสำคัญที่ทำไมผู้ถือบัตรต้องตรวจสอบและติดตามใบเรียกเก็บเงินที่เจ้าหนี้ควรต้องจัดส่งถึงตนภายในเวลาอันควร และแจ้งเจ้าหนี้ทันทีเมื่อปรากฏว่าตนไม่ได้รับใบเรียกเก็บเงินภายในกำหนด

2. หนังสือบอกกล่าวของผู้ถือบัตรต้องระบุข้อมูลที่ชัดเจนเพียงพอจะทำให้เจ้าหนี้สามารถรู้ได้ว่าเป็นข้อร้องเรียนของผู้ถือบัตรรายใด หมายเลขบัญชีใด และต้องมีเนื้อความที่สามารถเข้าใจได้ง่าย

3. ภายหลังการยื่นหนังสือบอกกล่าวแล้ว ผู้ถือบัตรอาจระงับการจ่ายเงินสำหรับรายการที่ยังคงมีข้อโต้แย้งกันอยู่

ขั้นตอนของเจ้าหนี้ภายหลังการได้รับหนังสือบอกกล่าว

1. เจ้าหนี้ต้องดำเนินการตรวจสอบรายการค่าใช้จ่ายตามที่มีการร้องเรียนว่ามีข้อผิดพลาด เว้นแต่เจ้าหนี้จะได้ตรวจสอบแก้ไขไปก่อนหน้านั้นแล้ว หรือผู้ถือบัตรได้ถอนคำร้องเรียนไปแล้ว

2. เจ้าหนี้ต้องจัดส่งหนังสือชี้แจงข้อร้องเรียนไปยังผู้ถือบัตรภายในกำหนด 30

วันนับแต่วันที่ได้รับหนังสือบอกกล่าว

3. ภายหลังที่เจ้าหนี้ได้รับหนังสือบอกกล่าวจากผู้ถือบัตรแล้ว เจ้าหนี้ต้องดำเนินการตามขั้นตอนการแก้ไขปัญหาภายใน 2 รอบระยะเวลาเรียกเก็บเงิน (แต่ไม่เกิน 90 วัน)

4. ขั้นตอนการแก้ไขปัญหา

ก. หากเจ้าหนี้พบว่ามีความผิดพลาดเกิดขึ้นตามข้อร้องเรียน เจ้าหนี้ต้องดำเนินการแก้ไขและเครดิตบัญชีของผู้ถือบัตรให้ถูกต้อง จากนั้นจัดส่งหนังสือแจ้งผลการแก้ไขไปยังผู้ถือบัตรเพื่อทราบ

ข. หากภายหลังการตรวจสอบไม่พบข้อผิดพลาดใด หรือพบข้อผิดพลาดที่แตกต่างไปจากข้อร้องเรียนของผู้ถือบัตร เจ้าหนี้ต้องจัดส่งหนังสือไปยังผู้ถือบัตรเพื่ออธิบายเหตุผลและรายละเอียดที่เกิดขึ้น ว่าความผิดพลาดที่ได้รับการบอกกล่าวมานั้นไม่ถูกต้องทั้งหมดหรือบางส่วน โดยเจ้าหนี้ต้องจัดส่งสำเนาหลักฐานยอดหนี้นั้นไปยังผู้ถือบัตรเพื่อตรวจสอบด้วย แล้วจึงแก้ไขข้อผิดพลาดและเครดิตบัญชีของผู้ถือบัตรให้ถูกต้อง

5. ขณะที่การเรียกเก็บเงินที่มีข้อผิดพลาดอยู่ในระหว่างการตรวจสอบแก้ไขภายใต้ขั้นตอนที่กำหนดไว้ใน FCBA นั้น ต้องปฏิบัติดังนี้

ก. เจ้าหนี้ไม่อาจ

- ดำเนินการเรียกเก็บเงินในจำนวนที่ยังคงมีข้อโต้แย้ง และหากเป็นกรณีที่ผู้ถือบัตรเปิดบัญชีเงินฝากไว้กับเจ้าหนี้โดยตกลงให้เจ้าหนี้สามารถหักค่าใช้จ่ายที่เกิดจากการใช้บัตรเครดิตออกจากเงินในบัญชีเงินฝากได้ เจ้าหนี้ก็ยังไม่อาจหักเงินจำนวนที่ยังคงมีข้อโต้แย้งได้หากเจ้าหนี้ได้รับหนังสือบอกกล่าวเป็นเวลา 3 วันทำการก่อนถึงวันครบกำหนดการชำระเงิน
- ตั้งข้อจำกัด หรือปิดบัญชีของผู้ถือบัตรด้วยเหตุที่ผู้ถือบัตรไม่ชำระเงินในจำนวนที่ยังคงมีข้อโต้แย้ง
- รายงานเครดิตของผู้ถือบัตรในทางเสื่อมเสียอันเนื่องจากจำนวนเงินที่ยังคงมีข้อโต้แย้ง

ข. หากภายหลังจากเจ้าหนี้ดำเนินการตามขั้นตอนการแก้ไขปัญหาแล้ว ผู้ถือบัตรยังคงร้องเรียนว่าข้อผิดพลาดยังคงมีอยู่ เจ้าหนี้อาจรายงานการไม่ชำระเงินนั้นไปยัง Credit Reporting Agency โดยระบุให้

- เจ้าหนี้ต้องรายงานจำนวนเงินที่ยังคงมีข้อโต้แย้ง

- จัดส่งหนังสือถึงผู้ถือบัตรเพื่อแจ้งชื่อและที่อยู่ของผู้ที่เจ้าหนี้มีรายงานไปถึง
- รายงานการแก้ไขปัญหาในครั้งหลังไปยังผู้ที่เจ้าหนี้มีรายงานไป ถึง

<u>ความรับผิดของผู้ถือบัตรจากการที่บัตรเครดิตของตนถูกใช้โดยปราศจากอำนาจ</u>

Truth in Lending Act (TILA) จำกัดความรับผิดของผู้ถือบัตร (Card Holder) ไว้ไม่เกิน 50 เหรียญสหรัฐต่อหนึ่งบัญชี[40] จากการที่บัตรเครดิตของตนถูกผู้อื่นนำไปใช้โดยปราศจากอำนาจ (Unauthorized Use) โดยเจ้าหนี้หรือผู้ออกบัตรต้องแจ้งข้อกำหนดเกี่ยวกับความรับผิดดังกล่าวนี้ให้ผู้ถือบัตรทราบก่อน รวมทั้งแจ้งให้ทราบถึงข้อปฏิบัติของผู้ถือบัตรหากเกิดกรณีบัตรเครดิตสูญหายหรือถูกขโมย ความรับผิดที่แตกต่างกันของผู้ถือบัตรในกรณีที่บัตรเครดิตของตนถูกใช้โดยปราศจากอำนาจในระยะเวลาก่อนและหลังที่ผู้ออกบัตรได้รับแจ้งการสูญหายหรือถูกขโมย การกระทำในลักษณะใดที่จะถูกอนุมานได้ว่าเป็นการใช้บัตรโดยมีอำนาจ

โดยทั่วไปแล้วหากการใช้บัตรโดยปราศจากอำนาจเกิดขึ้นภายหลังที่ผู้ถือบัตรได้แจ้งไปยังผู้ออกบัตรแล้วถึงการที่บัตรเครดิตของตนสูญหายหรือถูกขโมย ผู้ถือบัตรไม่ต้องรับผิดชอบต่อความเสียหายใดที่เกิดขึ้น ซึ่งภาระการพิสูจน์ว่าการใช้บัตรนั้นกระทำโดยมีหรือปราศจากอำนาจนั้น จะตกเป็นหน้าที่ของผู้ออกบัตร และหากเป็นการใช้บัตรโดยปราศจากอำนาจ ผู้ออกบัตรยังคงมีภาระการพิสูจน์ต่อไปด้วยว่าตนได้กำหนดเงื่อนไขให้ผู้ถือบัตรต้องรับผิดสำหรับค่าเสียหายส่วนแรกไว้ไม่เกิน 50 เหรียญสหรัฐและผู้ถือบัตรได้รับทราบเงื่อนไขดังกล่าวแล้ว

การใช้บัตรโดยปราศจากอำนาจ (Unauthorized Use) หมายถึง การที่ผู้อื่นนำบัตรเครดิตไปใช้โดยมิได้รับมอบอำนาจทั้งโดยตรงและโดยปริยายจากเจ้าของบัตรที่แท้จริง ซึ่งหลายรัฐได้ตีความคำว่า "Unauthorized Use" เพื่อคุ้มครองผู้ถือบัตรจากการใช้บัตรที่เกิดจากการสูญหาย ถูกขโมย หรือการกระทำผิดในลักษณะอื่นที่ใกล้เคียงเท่านั้น ตัวอย่างคดีระหว่าง Martin v. American Express,Inc.,361 So.2d 597 (Ala.CivApp.1978) ศาลได้ตัดสินว่าการที่ผู้ถือบัตรมอบอำนาจให้ผู้อื่นนำบัตรของตนไปใช้ในวงเงิน 500 เหรียญสหรัฐ แต่ผู้นั้นกลับนำไปใช้เกินวงเงิน ผู้ถือบัตรมีความรับผิดสำหรับค่าใช้จ่ายทั้งหมดที่เกิดขึ้น โดยไม่ถือว่าค่าใช้จ่ายในส่วนที่เกินวงเงินนั้นเกิดจากการใช้บัตรโดยปราศจากอำนาจ และในคดีระหว่าง Master Card v. Town of Newport,396 N.W.2d 345 (Wis.1986) ศาลได้ตัดสินในทำนองเดียวกันว่า การที่ผู้ถือบัตรมอบ

---

[40] 15 U.S.C.sec.1643

อำนาจให้ผู้อื่นนำบัตรของตนไปใช้เพื่อวัตถุประสงค์ใดโดยเฉพาะ แต่ผู้นั้นกลับนำบัตรไปใช้เพื่อวัตถุประสงค์อื่น การกระทำดังกล่าวไม่ถือเป็นการใช้บัตรโดยปราศจากอำนาจ ดังนั้น ผู้ถือบัตรจึงมีความรับผิด[41]

ตามบทบัญญัติของกฎหมายนี้ สามารถนำไปปรับใช้กับการที่คนร้ายนำหมายเลขบัตรเครดิตของผู้อื่นไปใช้บนอินเตอร์เนทโดยปราศจากอำนาจ ด้วยเหตุที่หมายเลขบัตรเครดิตที่คนร้ายได้มานั้น อาจได้มาจากการที่บัตรเครดิตของผู้อื่นสูญหาย ถูกขโมย หรือเกิดจากความผิดอื่นที่มีลักษณะใกล้เคียงกัน ดังนั้น เมื่อปรากฏว่ามีคนร้ายนำหมายเลขบัตรเครดิตของผู้อื่นไปใช้โดยปราศจากอำนาจบนอินเตอร์เน็ต จนเป็นเหตุให้มีการเรียกเก็บเงินที่มีข้อผิดพลาดเกิดขึ้น เจ้าของบัตรเครดิตที่แท้จริงย่อมมีหน้าที่ต้องปฏิบัติเพื่อให้ได้รับความคุ้มครองตามกฎหมายนี้[42]

สภาพปัญหาพาณิชย์อิเล็คทรอนิคส์ในประเทศอังกฤษ

นายโทนี แบลร์ นายกรัฐมนตรีของอังกฤษได้กล่าวคำปรารภไว้ว่า พาณิชย์อิเล็กทรอ นิกส์มีผลกระทบต่อระบบธุรกิจ รัฐบาล ผู้บริโภค และประชาชนโดยทั่วไป หลายประเทศใช้ประโยชน์อย่างเต็มที่จากพาณิชย์อิเล็คทรอนิคส์เพื่อการพัฒนาประเทศ โดยลดต้นทุนการผลิตต่างๆ ในการเข้าแข่งขันทางการค้ากับผู้ประกอบการต่างๆ ทั่วโลก หน่วยงาน Performance and Innovation Unit (PIU) ได้จัดเตรียมกลยุทธ์ที่จะทำให้ UK เป็นแหล่งพาณิชย์อิเล็คทรอนิคส์ที่ดีที่สุดในโลก PIU เห็นว่า UK อยู่ในระดับที่เหมาะสมอย่างมากที่จะบรรลุถึงเป้าหมายได้ เนื่องจากมีระบบการสื่อสารแบบเปิดกว้าง มีตลาดแข่งขันในระดับโลก มีระดับการใช้อินเตอร์เนททั้งในบ้านและสถานที่ทำงานค่อนข้างสูง และภาษาอังกฤษเป็นภาษาสากลที่ใช้กันในอินเตอร์เนท แต่อย่างไรก็ตามก็ยังไม่สามารถนิ่งนอนใจได้เพราะจากการสำรวจความเห็นของกรรมการบริษัทต่างๆ ใน UK พบว่ามีเพียงร้อยละ 2 ที่เชื่อว่าอินเตอร์เนทจะมีส่วนช่วยในการแข่งขันทางธุรกิจอย่างจริงจัง[43]

---

[41] ข้อมูลดังกล่าวแปลมาจาก Fair Credit Billing Act ใน Http://www.creditcardsearch engine.com/tips/fcba.html, (3 November 2000).

[42] ข้อมูลดังกล่าวแปลมาจาก ID Theft : When Bad Things Happen To Your Good Name ใน Http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm, (20 May 2001) และ U.S. Consumer Rights ใน Http://www.workz.com/content/275.asp, (12 July 2001).

[43] ข้อมูลดังกล่าวแปลมาจาก A Performance and Innovation Unit Report ใน Http:// www.e-commerce@its. best.uk, (20 May 2001).

องค์ประกอบสำคัญ 3 ประการที่จะพัฒนาพาณิชย์อิเล็คทรอนิคส์ใน UK และถือเป็นปัญหาสำคัญที่ควรได้รับการปรับปรุงแก้ไข คือ Understanding, Access และ Trust

1. การส่งเสริมความเข้าใจแก่ประชาชนทั่วไปให้รับรู้ถึงความสามารถของพาณิชย์อิเล็คทรอนิคส์ (Understanding)

1.1 ให้ประชาชนรับรู้ถึงประโยชน์ที่จะได้รับจากพาณิชย์อิเล็คทรอนิคส์ และรู้สึกเชื่อมั่นว่าเขามีความสามารถพอที่จะแสวงหาประโยชน์จากพาณิชย์อิเล็คทรอนิคส์ได้ และทุกคนในสังคมจะได้รับประโยชน์ร่วมกันจากการใช้พาณิชย์อิเล็คทรอนิคส์

1.2 ให้ประชาชนสามารถใช้สื่ออิเล็คทรอนิคส์ต่างๆ ในการติดต่อทำธุรกรรมกับหน่วยงานต่างๆ ของภาครัฐโดยได้รับผลไม่แตกต่างจากการติดต่อด้วยวิธีปกติ เช่น การขอและต่ออายุใบอนุญาตขับขี่, การต่ออายุหนังสือเดินทาง และการจดทะเบียนจัดตั้งบริษัท เป็นต้น

1.3 ให้ประชาชนเข้าใจว่าพาณิชย์อิเล็คทรอนิคส์ถูกนำมาใช้เพื่อลดต้นทุน และเสริมสร้างระบบธุรกิจและอุตสาหกรรมใหม่บนออนไลน์

1.4 พัฒนาทักษะและการศึกษาพาณิชย์อิเล็คทรอนิคส์แก่ลูกจ้างทั้งหมดอย่างสม่ำเสมอ ทั้งที่บ้านและที่ทำงาน

2. ความสะดวกในการเข้าถึงเทคโนโลยีและเครือข่าย (Access)

2.1 จัดให้มีเทคโนโลยีและสื่ออิเล็คทรอนิคส์ต่างๆ ที่มีคุณภาพสูงและเสียค่าใช้จ่ายน้อย เพื่อให้ประชาชนทั่วไปได้เข้าถึงกันอย่างแพร่หลาย

2.2 จัดให้มีการเข้าถึงพาณิชย์อิเล็คทรอนิคส์โดยไม่จำกัด รวมทั้งในส่วนที่เป็นของภาครัฐ ทั้งนี้ไม่ว่าจะเป็นการเข้าถึงจากบ้านหรือศูนย์บริการต่างๆ

2.3 สร้างระบบรูปภาพและเสียงเข้ามาเป็นส่วนประกอบ เพื่อช่วยลดอุปสรรคจากการที่ไม่สามารถอ่านข้อความได้เข้าใจ

3. ความน่าเชื่อถือ (Trust)

3.1 ประชาชนทั่วไปต้องสามารถใช้เครือข่ายเพื่อการพาณิชย์อิเล็คทรอนิคส์ โดยมีความเสี่ยงน้อยที่สุดจากการถูกฉ้อโกง

3.2 สามารถใช้ข้อมูลส่วนตัวในการทำพาณิชย์อิเล็คทรอนิคส์ โดยมีความเสี่ยงน้อยจากการถูกขโมยข้อมูล

3.3 กำหนดความรับผิดและกระบวนการแก้ไขชดใช้ค่าเสียหาย ในกรณีที่มีข้อผิดพลาดเกิดขึ้น

3.4 ควบคุมเนื้อหาสารสนเทศที่อยู่บนเครือข่ายให้อยู่ในความเหมาะสม

3.5 มีระบบเทคโนโลยีที่เข้ามาช่วยลดความเสี่ยงได้อย่างแท้จริงจากการที่ข้อมูลจะถูกขโมยหรือถูกทำให้เสียหาย

3.6 มีความเสี่ยงน้อยจากการถูกขโมยทรัพย์สินทางปัญญา

กฎหมายของประเทศอังกฤษ

1. Theft Act of 1968[44]

ความผิดเกี่ยวกับการได้รับทรัพย์สินมาโดยการหลอกลวง ถูกบัญญัติไว้ในมาตรา 5 ซึ่งมีสาระสำคัญ ดังนี้

1. บุคคลใดผู้ซึ่งได้รับทรัพย์สินของบุคคลอื่นโดยไม่สุจริต หลอกลวงด้วยเจตนาที่จะไม่ต้องการให้ผู้อื่นมาเกี่ยวข้องกับทรัพย์สินนั้น จะมีความผิดและถูกลงโทษจำคุกไม่เกินสามปี

2. บุคคลที่ได้รับทรัพย์สิน คือ บุคคลที่ได้รับความเป็นเจ้าของ ความครอบครองหรือการควบคุมทรัพย์นั้น และการได้รับ รวมถึงการได้รับเพื่อบุคคลอื่น หรือทำให้บุคคลอื่นสามารถได้รับหรือรักษาไว้

3. การหลอกลวง หมายถึง การหลอกลวงไม่ว่าโดยตั้งใจหรือประมาท โดยคำพูดหรือการกระทำซึ่งเป็นข้อเท็จจริง หรือตามกฎหมาย รวมถึงการหลอกลวงที่จะแสดงถึงเจตนาของบุคคลที่ใช้การหลอกลวงนั้นหรือบุคคลอื่นใด

---

[44] Smith & Hogan, Criminal Law,6th ed., (Butterworths, 1988), pp.557-558.

บทบัญญัติในกฎหมายของประเทศอังกฤษในส่วนที่เกี่ยวข้องกับการนำหมายเลขบัตรเครดิตของผู้อื่นไปใช้โดยปราศจากอำนาจนั้นมิได้ถูกบัญญัติไว้เป็นการเฉพาะ แต่เมื่อพิจารณาถึงลักษณะของการกระทำความผิด จะเห็นได้ว่าผู้ที่นำหมายเลขบัตรเครดิตของผู้อื่นไปใช้สั่งสินค้าและบริการบนอินเตอร์เนทนั้น ย่อมคาดหวังที่จะได้รับทรัพย์สินจากร้านค้าหรือสถานบริการดังกล่าว ซึ่งการนำหมายเลขบัตรเครดิตของผู้อื่นไปกรอกลงบนหน้าจอคอมพิวเตอร์ก็เป็นรูปแบบหนึ่งของการหลอกลวงร้านค้า เพื่อให้หลงเชื่อว่าหมายเลขบัตรเครดิตนั้นเป็นของตน หรือตนเป็นผู้ที่มีอำนาจใช้ ดังนั้น เมื่อคนร้ายได้รับทรัพย์สินของผู้อื่นมาโดยการหลอกลวงย่อมถือเป็นความผิดตามกฎหมายนี้

2. Computer Misuse Act of 1990

เทคโนโลยีทางคอมพิวเตอร์ส่งผลกระทบต่อกฎหมายอาญา 2 ประการ ประการแรก คือ ก่อให้เกิดความสะดวกในการก่ออาชญากรรมที่เป็นอยู่ในขณะนี้ เช่น การฉ้อโกง การลักทรัพย์ ประการที่สอง คือ ก่อให้เกิดรูปแบบใหม่ของการกระทำความผิด เช่น การเจาะระบบข้อมูล (hacking) การแพร่กระจายไวรัส ซึ่งการกระทำโดยส่วนใหญ่เกิดขึ้นจากลูกจ้างหรือพนักงานภายในองค์กรนั้นๆ

รูปแบบหนึ่งของอาชญากรรมทางคอมพิวเตอร์ คือ การเข้าไปล่วงละเมิดต่อข้อมูลหรือความเป็นส่วนตัวของผู้อื่นโดยการเจาะระบบ (Hacking) ดังนั้น กฎหมายที่เข้ามาคุ้มครองความเป็นส่วนตัวของผู้อื่นที่เก็บอยู่ในระบบคอมพิวเตอร์จึงมีความจำเป็นอย่างยิ่ง ประเทศอังกฤษได้กำหนดความผิดสำหรับการเข้าสู่ระบบคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจไว้ โดยเปรียบเทียบกับความผิดฐานบุกรุกและความผิดเกี่ยวกับทรัพย์สิน ซึ่งแต่เดิมการ Hacking ไม่ถือเป็นความผิดทางอาญา[45] คงเป็นความผิดในทางแพ่งเท่านั้น จึงมีการบัญญัติกฎหมายโดยกำหนดให้การเข้าสู่ระบบประมวลผลโดยปราศจากอำนาจเป็นความผิดอาญา ไม่ว่าผู้ที่เข้าสู่ระบบประมวลผลจะเป็น Hacker หรือไม่ ซึ่งอาจเป็นลูกจ้างที่ไม่มีอำนาจที่จะเข้าไป หรือบุคคลภายนอกก็ตาม

ในปี ค.ศ.1990 ประเทศอังกฤษได้มีการออกกฎหมาย Computer Misuse Act of 1990 (CMA) กฎหมายฉบับนี้ได้จัดลำดับความผิดของการใช้ระบบคอมพิวเตอร์ไว้ แต่เดิมในช่วงปี

---

[45] เฉลิมพล ซ่อโพธิ์ทอง, "ความผิดฐานลักทรัพย์และฉ้อโกง : ศึกษาเปรียบเทียบกฎหมายอังกฤษ เยอรมัน และไทย" (วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชานิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ . 2535), หน้า 73.

ค.ศ.1980 การเจาะระบบ (Hacking) ไม่ถือว่าเป็นความผิด ดังนั้น Hacker จึงมีอิสระในการเข้าสู่ระบบคอมพิวเตอร์ของผู้อื่นถ้าหากเขามีความสามารถในการผ่านระบบรักษาความปลอดภัยของเจ้าของระบบเข้าไปได้ ซึ่งในขณะนั้นบางคนมองว่าเป็นเพียงการรบกวนเล็กน้อย หรือเป็นเรื่องของความกล้าท้าทาย แต่บางคนมองว่าการกระทำดังกล่าวเป็นภัยต่อสังคม เพราะการเจาะระบบสามารถพัฒนาไปสู่การกระทำบางสิ่งอันเกี่ยวกับคอมพิวเตอร์ที่รุนแรงมากขึ้นและเป็นภัยต่อสังคม ในขณะที่กฎหมายที่มีอยู่ในขณะนั้นไม่มีประสิทธิภาพเพียงพอที่จะจำกัดการกระทำของ Hacker

ก่อนที่ CMAจะถูกบัญญัติขึ้น การทำให้เกิดความเสียหายหรือการลบโปรแกรมหรือข้อมูลทางคอมพิวเตอร์ถือเป็นความผิดภายใต้มาตรา 1 ของ The Criminal Damage Act of 1971 หรือ CDA ซึ่งบัญญัติว่า "บุคคลจะถูกถือว่ามีความผิด ถ้าผู้นั้นได้ทำลายหรือทำให้เสียหายซึ่งทรัพย์สินที่เป็นของผู้อื่น โดยปราศจากข้ออ้างตามกฎหมาย" ความเสียหายทางอาญาตาม CDA วางหลักว่า ผู้กระทำต้องมีเจตนาให้ผลนั้นเกิดขึ้น หรือประมาทจนเป็นเหตุให้ทรัพย์สินของผู้อื่นถูกทำลาย หรือทำให้เสียหาย ซึ่งอุปสรรคในการปรับบทกฎหมายนี้ก็คือถ้อยคำที่ว่า "Property must be destroyed or damaged" เพราะคำว่า "Property" ได้มีการจำกัดความไว้ในมาตรา 10 ของ CDA ว่า หมายถึง ทรัพย์ที่มีรูปร่างเท่านั้น ซึ่งดูเหมือนจะไม่รวมถึง data หรือ software อันเป็นผลให้ศาลในบางคดีต้องหาทางออกอื่นในการลงโทษจำเลย ดังเช่น คดี Cox v Riley (1986) 83 Cr App R 54 จำเลยได้ลบโปรแกรมจาก print circuit card ซึ่งใช้สำหรับควบคุมระบบคอมพิวเตอร์ของเลื่อยยนต์ตัดไม้ของนายจ้าง ทำให้เครื่องมือนั้นไม่สามารถใช้งานได้ จำเลยถูกฟ้องภายใต้กฎหมาย CDA จำเลยต่อสู้ว่าโปรแกรมดังกล่าวไม่ใช่ทรัพย์ที่มีรูปร่างภายใต้ความหมายของ CDA แต่ศาลได้ตัดสินว่าจำเลยมีความผิด ซึ่งศาลได้หาทางออกโดยใช้เหตุผลว่าเครื่องมือนั้นได้ถูกทำให้เสียหายและไร้ประโยชน์

ในคดี Whiteley (1991) 93 Cr App R 25 จำเลยคือ Nicolas Whiteley อายุ 21 ปี ผู้ที่รู้จักกันดีในนาม "Mad-Hacker" ถูกฟ้อง 10 กระทง ในข้อหาเจตนาหรือโดยประมาทเป็นเหตุให้ทรัพย์สินของผู้อื่นเสียหาย โดยจำเลย hack เข้าไปในเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยหลายแห่งผ่านทางเครือข่ายทางการศึกษา (Joint Academic Network / JANET) ในช่วงระหว่างเดือนมีนาคมถึงเดือนกรกฎาคม 1988 เขาได้ลบ เพิ่ม และสร้างระบบผู้ใช้ของเขาเอง รวมถึงจัดการให้ได้มาซึ่งอำนาจในการจัดการระบบคอมพิวเตอร์ ซึ่งการกระทำดังกล่าวก่อให้เกิดผลทำให้ระบบคอมพิวเตอร์ล้มเหลว และไม่สามารถทำงานได้อย่างปกติ เขาถูกตัดสินว่ามีความผิด โดย Lord Lane CJ ได้กล่าวว่า อนูของแม่เหล็ก (magnetic particles) ที่อยู่ในแผ่นโลหะ (metal disc) ถือเป็นส่วนหนึ่งของแผ่นโลหะนั้น และหากพิสูจน์ได้ว่าจำเลยเป็นผู้ทำการเปลี่ยนแปลงอนูในทางที่

ได้สร้างความเสียหายต่อคุณค่าหรือการใช้ประโยชน์ของแผ่นโลหะนั้น ย่อมถือเป็นความเสียหายภายใต้มาตรา 1 ของ CDA ไม่ว่าความเสียหายนั้นจะเป็นการชั่วคราวหรือถาวร ซึ่งในคดีลักษณะเช่นเดียวกันนี้ หากเกิดขึ้นภายหลังที่กฎหมาย Computer Misuse Act (CMA) ใช้บังคับแล้วจะอยู่ภายใต้ความผิดฐานเปลี่ยนแปลงแก้ไขระบบคอมพิวเตอร์โดยปราศจากอำนาจ ตามมาตรา 3

นอกจากนี้ ตามกฎหมายดั้งเดิมของประเทศอังกฤษนั้น ความผิดฐานลักทรัพย์ตามมาตรา 1-6 ของ Theft Act of 1968 วางหลักว่า "บุคคลจะมีความผิดฐานลักทรัพย์ ถ้าเขาครอบครองทรัพย์ของผู้อื่นโดยทุจริต โดยเจตนาตัดสิทธิทรัพย์นั้นไปอย่างถาวร" บทบัญญัติดังกล่าวก่อให้เกิดประเด็นทางกฎหมายที่ควรปรับปรุงแก้ไขเพื่อนำไปใช้กับอาชญากรรมคอมพิวเตอร์ เช่น

- ควรให้คำจำกัดความคำว่า "ทรัพย์" อย่างกว้างขวาง เพื่อสามารถนำไปปรับใช้ได้กับทุกๆ สิ่ง
- ทรัพย์จะถูกถือว่าเป็นของบุคคลอื่น ถ้าบุคคลนั้นมีสิทธิในทรัพย์สินนั้นตามกฎหมายหรือเพียงแต่มีอำนาจควบคุมก็เพียงพอแล้ว
- การครอบครองให้สันนิษฐานไว้ก่อนว่ามีสิทธิเป็นเจ้าของ

บทบัญญัติของกฎหมายเดิมที่มีอยู่ก่อให้เกิดปัญหาในการปรับใช้กฎหมายกับความผิดต่างๆ ที่เกิดขึ้นอันเกี่ยวกับระบบคอมพิวเตอร์ ส่งผลให้ผู้พิพากษาในแต่ละคดีต้องตีความกฎหมายไปในรูปแบบต่างๆ ตามแนวทางของตน ทั้งนี้ก็เพื่อให้ได้ตัวผู้กระทำผิดมาลงโทษ ปัญหาต่างๆ ที่เกิดขึ้น ได้แก่ คำว่า "ทรัพย์" ซึ่งตามแนวความคิดดั้งเดิมนั้นหมายถึงวัตถุที่มีรูปร่าง มีลักษณะทางกายภาพอย่างเห็นได้ชัด และความเสียหายที่เกิดขึ้นต้องเป็นความเสียหายที่ปรากฏทางกายภาพ นอกจากนี้ การได้รับโดยการหลอกลวง (obtaining by deception) ซึ่งถือเป็นส่วนหนึ่งของความผิดฐานฉ้อโกงนั้น ถูกบัญญัติไว้ใน section 15 (1) ของ The Theft Act of 1968 ว่า "ผู้ใดโดยทุจริตได้ทำการหลอกลวงเพื่อให้ได้รับทรัพย์สินซึ่งเป็นของผู้อื่น โดยมีเจตนาแย่งการครอบครองไปอย่างถาวร ต้องระวางโทษ" องค์ประกอบสำคัญของความผิดฐานนี้ คือ ต้องเป็นมนุษย์เท่านั้นจึงจะถูกหลอกลวงได้

จากปัญหาและอุปสรรคต่างๆ ในการบังคับใช้กฎหมายเดิมที่มีอยู่นั้น จึงมีการจัดตั้ง A Royal Commission ขึ้นมาเพื่อตรวจสอบถึงปัญหาการใช้คอมพิวเตอร์ในทางมิชอบ จากผลการตรวจสอบและคำแนะนำของ A Royal Commission ก่อให้เกิดการร่างกฎหมาย

Computer Misuse Act of 1990 ขึ้นมาเพื่อยุติปัญหาต่างๆ ที่เกิดขึ้น หลักสำคัญของกฎหมายดังกล่าวที่จะนำมาพิจารณาแบ่งเป็น 3 ส่วน ดังนี้

ส่วนที่ 1 เป็นบทบัญญัติขั้นพื้นฐาน ใช้สำหรับการกระทำความผิดที่ไม่ซับซ้อน ดังปรากฏอยู่ในมาตรา 1 ซึ่งบัญญัติว่า

(1) บุคคลมีความผิด ถ้า

(a) ผู้นั้นได้ทำการให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ โดยความจงใจที่จะผ่านสิ่งที่ปกป้องคุ้มครองไม่ให้เข้าสู่ระบบได้ และได้ผ่านสิ่งปกป้องเช่นว่านั้นเข้าไปยังโปรแกรมใดๆ หรือข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ใดๆ

(b) การผ่านสิ่งปกป้องคุ้มครองเข้าไปสู่ระบบด้วยความจงใจนั้นเป็นการกระทำโดยปราศจากอำนาจ และ

(c) ผู้นั้นได้รู้อยู่ในเวลาที่เขาได้กระทำการอันเป็นเหตุให้คอมพิวเตอร์นั้นแสดงผล หรือแสดงการทำงานอันปราศจากอำนาจนั้น

(2) ความจงใจของบุคคลที่ได้กระทำความผิดภายใต้มาตรานี้ ไม่จำเป็นต้องเป็นการกระทำที่เป็น

(a) โปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล

(b) โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือ

(c) โปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์อย่างเฉพาะเจาะจง

(3) บุคคลที่มีความผิดภายใต้บทบัญญัตินี้จะต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ การพิจารณาคดีตามความผิดนี้ให้พิจารณาแบบรวบรัด

องค์ประกอบในส่วนของการกระทำตามมาตรานี้ กำหนดให้ผู้กระทำผิดจะต้องกระทำการอันเป็นเหตุให้คอมพิวเตอร์แสดงผลการทำงานใดๆ แต่ไม่ได้หมายความถึงกรณีที่เพียงแต่สัมผัสทางกายภาพกับเครื่องคอมพิวเตอร์และวิเคราะห์ข้อมูลโดยไม่ได้มีการโต้ตอบใดๆ กับเครื่องคอมพิวเตอร์ ดังนั้น การอ่านข้อมูลที่แสดงผลบนหน้าจอ หรือการดักจับข้อมูล การดักฟังข้อมูล จึงไม่อยู่ในข่ายของความผิดตามมาตรานี้ และการที่ผู้กระทำจะต้องรับผิดนั้นไม่จำเป็นว่าผู้กระทำจะประสบผลสำเร็จในการเข้าสู่ระบบประมวลผล เข้าสู่โปรแกรมหรือข้อมูลหรือไม่ ก็ถือเป็นความผิดสำเร็จแล้ว

สาระสำคัญของมาตรานี้มุ่งเน้นที่จะใช้กับการพยายามกระทำความผิด เพื่อให้การลงโทษมีประสิทธิภาพ ซึ่งคณะกรรมการร่างกฎหมายได้ใช้คำว่า "knocking on the door of the computer" ซึ่งหมายความว่า Hacker ต้องกระทำการเพื่อพังประตูที่ปิดกั้นทางเข้าสู่ระบบคอมพิวเตอร์นั้น ไม่ว่าจะประสบความสำเร็จหรือไม่ อันถือเป็นการรับผิดเด็ดขาด

องค์ประกอบทางด้านจิตใจ แบ่งออกเป็น 2 ประการ

1. เจตนาที่จะผ่านสิ่งปกป้องคุ้มครองระบบเพื่อเข้าสู่โปรแกรมใดๆ หรือข้อมูลที่อยู่ในคอมพิวเตอร์ใด ๆ กล่าวคือ เจตนานั้นไม่จำเป็นต้องมีความสัมพันธ์กับคอมพิวเตอร์ที่ผู้กระทำผิดเปิดเครื่องปฏิบัติการอยู่ในเวลานั้น โดยในอนุมาตรา 2 อธิบายคำว่าเจตนาของผู้กระทำผิดว่าไม่จำเป็นต้องเป็นเจตนาโดยตรงที่มุ่งต่อการกระทำที่เป็นโปรแกรมเฉพาะเจาะจงใดๆ หรือข้อมูลใดๆ นั่นหมายความว่าหากเจตนากระทำต่อโปรแกรมใดๆ ก็เป็นความผิด ทั้งนี้เพื่อให้รวมความถึง Hacker ประเภทที่เข้าสู่ระบบโดยยังไม่มีความมุ่งหมายที่ชัดเจนในตอนแรกว่าจะเข้าไปทำอะไร แต่อาจคิดได้ภายหลังที่เข้าไปแล้ว

2. เจตนาภายใน คือ ผู้กระทำผิดต้องรู้ว่าขณะที่เขากระทำการอันเป็นเหตุให้เครื่องคอมพิวเตอร์แสดงผลหรือทำงานขึ้นนั้น เขาได้เข้าไปสู่ระบบโดยจงใจและปราศจากอำนาจ กล่าวคือ โจทก์ต้องพิสูจน์ให้ได้ว่าจำเลยมีเจตนาเข้าสู่ระบบ และจำเลยรู้อยู่ในขณะที่ทำให้เครื่องแสดงผลว่าเขาได้เข้าไปโดยจงใจและปราศจากอำนาจ ซึ่งอาจก่อให้เกิดข้อถกเถียงกันได้ว่า หากเป็นกรณีพนักงานหรือลูกจ้างในองค์กรต่างๆ กระทำการเข้าสู่ระบบ ควรจะต้องรับโทษเช่นเดียวกับ Hacker หรือไม่ เพราะการพิจารณาลงโทษจะต้องพิจารณาถึงการมีอำนาจในการเข้าสู่ระบบเสียก่อนว่ามีอำนาจหรือไม่ และที่เป็นปัญหาก็คือใครจะเป็นผู้มีอำนาจในการอนุญาต เพราะหากกำหนดหลักเกณฑ์ไว้ตายตัวก็จะก่อให้เกิดปัญหายุ่งยากในการปฏิบัติงาน

ศาลที่มีอำนาจพิจารณาคดีในความผิดตามมาตรา 1 นี้ คือ Magistrate Court ซึ่งตามมาตรานี้ได้กำหนดโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5,000 ปอนด์ หรือทั้งจำทั้งปรับ นอกจากนี้มาตรา 44 (1) แห่ง Magistrate's Court Act 1980 ยังเป็นบทบัญญัติที่ช่วยเสริมความผิดในส่วนนี้ กล่าวคือการลงโทษบุคคลที่ช่วยเหลือ Hacker โดยให้ความรู้ข้อมูลข่าวสาร รหัสผ่าน วิธีเข้าสู่ระบบเพื่อ Hacker จะสามารถผ่านเข้าสู่ระบบไปยังข้อมูลได้

ส่วนที่ 2 ใช้บังคับกับความผิดที่ซับซ้อนขึ้น ดังที่บัญญัติไว้ในมาตรา 2 ว่า

(1) บุคคลจะมีความผิดภายใต้บทบัญญัตินี้ ถ้าหากว่าเขาได้กระทำความผิดตามมาตรา 1 ด้วยเจตนา

(a) ได้กระทำผิดในสิ่งที่มาตรานี้บังคับใช้ หรือ

(b) ให้ความสะดวกในการกระทำผิดอื่น (ไม่ว่าโดยตนเองหรือบุคคลใด) และความผิดที่เขาจงใจกระทำหรือให้ความสะดวกดังจะกล่าวต่อไปในมาตรานี้ ให้ถือว่าเป็นผู้กระทำผิดเช่นเดียวกันกับผู้กระทำผิดที่ตนช่วย

(2) มาตรานี้ใช้กับความผิด

(a) ใช้กับความผิดที่ถูกกำหนดไว้โดยกฎหมาย หรือ

(b) ใช้กับบุคคลผู้มีอายุ 21 ปีขึ้นไป

(3) เพื่อวัตถุประสงค์ของมาตรานี้ ไม่ว่าการกระทำความผิดของผู้กระทำที่อยู่ห่างไกล (Remote Hacker) จะได้กระทำลงในโอกาสที่ไม่มีอำนาจในการเข้าสู่ระบบนั้นหรือไม่ หรือโดยอาศัยโอกาสอื่นใดก็ตาม

(4) บุคคลอาจจะมีความผิดตามมาตรานี้ ถึงแม้ว่าจะมีข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำที่อยู่ห่างไกลจะไม่ได้กระทำลงก็ตาม

(5) บุคคลผู้กระทำผิดตามมาตรานี้จะต้องรับผิด

(a) จะพิจารณาคดีแบบรวบรัด และถูกลงโทษจำคุกไม่เกิน 6 เดือน หรือปรับ หรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงจะถูกลงโทษไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ

กรณีตามมาตรา 2 เป็นความผิดที่อาจอยู่ในอำนาจของ Crown Court หรือ Magistrate Court ก็ได้ขึ้นอยู่กับความร้ายแรงของการกระทำความผิด มาตรา 2 ใช้ในความผิดประเภทที่ร้ายแรง หรือที่เป็นการกระทำความผิดโดยจงใจ หรือให้ความสะดวกแก่ผู้กระทำความผิดเพื่อก่อให้เกิดการกระทำความผิดร้ายแรงเกิดขึ้น สำหรับความผิดอื่นที่เรียกว่า further offence นั้น เป็นความผิดประเภทที่ไม่จำเป็นต้องพิสูจน์ถึงเจตนาของผู้กระทำว่าตนมีเจตนากระทำผิดขึ้นจริงหรือไม่ แต่ความผิดอื่นนี้ต้องเป็นความผิดที่มีโทษจำคุกตามกฎหมาย เช่น การฆาตกรรม หรือมีโทษจำคุกไม่ต่ำกว่า 5 ปี ซึ่งสามารถปรับใช้ได้กับการได้รับทรัพย์สินหรือบริการไปโดยการหลอกลวง นอกจากนี้ยังต้องพิจารณาถึงหลัก Double Criminality ด้วย กล่าวคือ หากผู้กระทำผิดดำเนินการภายในสหราชอาณาจักร (UK) โดยมีเจตนาจะกระทำความผิดอื่นตามมาตรา 2 ในอีกประเทศหนึ่ง ความผิดอื่นนั้นต้องเป็นความผิดอาญาในประเทศนั้นด้วย

ความผิดตามมาตรา 1 เป็นกรณีที่ใช้กับการที่ไม่อาจพิสูจน์เจตนาในอนาคตได้ ซึ่งจะมีโทษเบากว่า แต่หากพิสูจน์เจตนาในอนาคตได้ให้ใช้มาตรา 2 ซึ่งเป็นหลักเกณฑ์ที่เทียบเคียงมาจากการพยายามกระทำความผิดใน Criminal Attempt Act 1981 มาตรา 1(2)[46]

ส่วนที่ 3 ปรากฏอยู่ในมาตรา 3 ดังนี้

(1) บุคคลจะมีความผิดถ้า

a) ผู้นั้นกระทำการใดอันเป็นเหตุให้มีการแก้ไขเปลี่ยนแปลงเนื้อหาของระบบคอมพิวเตอร์ใดๆ โดยปราศจากอำนาจ และ

b) ในขณะที่กระทำการนั้น ผู้กระทำมีเจตนาพิเศษและความรับรู้พิเศษ

(2) เจตนาพิเศษ คือ เจตนาที่จะก่อให้เกิดการแก้ไขเปลี่ยนแปลงต่อเนื้อหาของระบบคอมพิวเตอร์ และโดยการกระทำเช่นนั้น

a) ทำให้เสียหายต่อการทำงานของระบบคอมพิวเตอร์

b) ขัดขวางการเข้าถึงโปรแกรมหรือข้อมูลที่มีอยู่ในคอมพิวเตอร์ หรือ

c) ทำให้เสียหายต่อการทำงานของโปรแกรม หรือความน่าเชื่อถือของข้อมูล

(3) เจตนาไม่จำเป็นต้องกระทำโดยตรงต่อ

a) คอมพิวเตอร์เครื่องหนึ่งเครื่องใดเป็นการเฉพาะ

b) โปรแกรมหรือข้อมูลใดเป็นการเฉพาะ หรือ

c) การแก้ไขเปลี่ยนแปลงในรูปแบบใดรูปแบบหนึ่งโดยเฉพาะ

(4) ความรับรู้พิเศษ คือ รู้ว่าการแก้ไขเปลี่ยนแปลงที่ผู้กระทำมีเจตนากระทำนั้นกระทำโดยปราศจากอำนาจ

(5) ภายใต้มาตรานี้ไม่จำเป็นต้องพิจารณาว่า การแก้ไขเปลี่ยนแปลงโดยปราศจากอำนาจ ผู้กระทำจะมุ่งให้เกิดผลของการกระทำโดยชั่วคราวหรือถาวร

(6) เพื่อให้สอดคล้องกับ The Criminal Damage Act 1971 การแก้ไขเปลี่ยนแปลงเนื้อหาของคอมพิวเตอร์จะไม่ถูกถือว่าได้สร้างความเสียหายต่อคอมพิวเตอร์ เว้นแต่ผลกระทบนั้นจะส่งผลทางกายภาพ

---

[46] สุเนติ คงเทพ, "การไม่มีอำนาจเข้าสู่ระบบประมวลผล (Hacking)," บทบัณฑิตย์. เล่ม 55 ตอน 1 (มีนาคม 2542) : หน้า 134-138.

(7) บุคคลผู้กระทำผิดตามมาตรานี้จะต้องรับผิด

(a) จะพิจารณาคดีแบบรวบรัด และถูกลงโทษจำคุกไม่เกิน 6 เดือน หรือปรับหรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงจะถูกลงโทษไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ

คำว่า "การแก้ไขเปลี่ยนแปลง" (Modification) ถูกให้คำจำกัดความไว้ในมาตรา 17 ว่าหมายถึง การเปลี่ยนแปลง ลบ เพิ่ม ที่กระทำต่อโปรแกรมหรือข้อมูล ซึ่งรวมถึงไวรัสคอมพิวเตอร์ด้วย เช่น worm, trojan horses, logic bombs

กฎหมายฉบับนี้ได้วางหลักเกณฑ์ในเรื่องเขตอำนาจศาลไว้ในมาตรา 4-9 เนื่องจากก่อนหน้านี้ในคดี R v Tomsett (1985) ซึ่งเป็นเรื่องที่จำเลยส่งเทเล็กซ์จากลอนดอนโดยเจตนาที่จะโอนเงินจากนิวยอร์คไปยังบัญชีของจำเลยในเจนีวา ศาลอุทธรณ์ตัดสินว่าหากการพยายามบรรลุผล การลักทรัพย์ดังกล่าวจะถูกถือว่าเกิดขึ้นในนิวยอร์ค ซึ่งศาลอังกฤษจะไม่มีอำนาจพิจารณาคดี เนื่องจากตามแนวคิดของกฎหมาย Common law พิจารณาจากผลของการกระทำว่าเกิดขึ้นที่ใด โดยมิได้มุ่งเน้นถึงสถานที่ที่ความผิดได้ถูกกระทำขึ้น ดังนั้น เพื่อป้องกันปัญหาที่จะเกิดขึ้น ภายใต้กฎหมายนี้จึงกำหนดในเรื่องความสัมพันธ์เอาไว้ ซึ่งระบุว่าความผิดที่อยู่ในเขตอำนาจศาลอังกฤษต้องเกิดจากการกระทำในหรือมุ่งต่อระบบคอมพิวเตอร์ใน Home Country ซึ่งหมายถึง อังกฤษ เวลส์ สก็อตแลนด์ และไอร์แลนด์เหนือ ที่รวมเรียกว่าสหราชอาณาจักร หรือ UK ความผิดที่อยู่ภายใต้บังคับของกฎหมายนี้ต้องเป็นความผิดที่เกิดขึ้นใน UK เช่น บุคคลจากอังกฤษกระทำการฉ้อโกงทางระบบคอมพิวเตอร์ในประเทศฟินแลนด์ ก็จะถูกถือว่ากระทำความผิดภายใต้กฎหมายฉบับนี้ ทั้งนี้ ส่วนหนึ่งส่วนใดของการกระทำที่เกิดขึ้นภายใน UK ต้องเป็นส่วนที่เป็นสาระสำคัญให้ผลของการกระทำความผิดนั้นเกิดขึ้น

Computer Misuse Act of 1990 ถูกบัญญัติขึ้นมาเพื่อป้องการการเข้าถึง (access) โดยปราศจากอำนาจ และมิให้อาชญากรรมที่เกิดจากการใช้คอมพิวเตอร์เป็นเครื่องมือช่วยเหลือในการกระทำความผิด หรือสร้างความเสียหาย หรือขัดขวางการเข้าถึงข้อมูลที่บรรจุในระบบคอมพิวเตอร์มีจำนวนเพิ่มมากขึ้นในสังคม อาชญากรรมคอมพิวเตอร์หลายรูปแบบที่ถูกศาลตัดสินว่าเป็นความผิดภายใต้กฎหมายฉบับนี้ ดังตัวอย่างคดี Denco Ltd v Joinson (1991) จำเลยซึ่งเป็นพนักงานของบริษัทแห่งหนึ่งทำการ hack โดยใช้คอมพิวเตอร์ของที่ทำงานในการเข้าถึงโปรแกรมหรือข้อมูลของผู้อื่นทั้งๆ ที่รู้ว่าตนไม่มีอำนาจในการเข้าถึง ศาลได้ตัดสินว่าลูกจ้างซึ่งใช้

password โดยไม่ได้รับอนุญาต เพื่อการเข้าถึงข้อมูลที่เก็บไว้ในคอมพิวเตอร์ เป็นผู้ประพฤติชั่ว และสามารถถูกไล่ออกจากงานได้

ในเดือนธันวาคม 1993 จำเลยซึ่งเป็นพยาบาลได้ hack เข้าสู่ระบบคอมพิวเตอร์ของโรงพยาบาลแห่งหนึ่ง และทำการแก้ไขเปลี่ยนแปลงรายการรวมทั้งใบสั่งยา โดยจำเลยสามารถเข้าสู่ระบบคอมพิวเตอร์ของโรงพยาบาลได้เนื่องจากสังเกตจากแพทย์ในขณะทำการ log in เข้าระบบคอมพิวเตอร์ หลังจากนั้นจำเลยได้สั่งยาให้แก่คนไข้ ศาลตัดสินจำคุก 12 เดือน

เมื่อวันที่ 26 มิถุนายน 1991 ตำรวจได้จับชาย 3 คน ซึ่งร่วมกัน hack ข้อมูลของมหาวิทยาลัยและของรัฐบาลทั่วโลก พวกเขาเรียกตัวเองว่า "Eight Legged Groove Machine (8LGM)" พวกเขาทิ้งข้อความเอาไว้ในระบบที่ถูก hack ว่า 8LGM หรือ "Eight little green men" พวกเขาไม่รู้จักกันเองแม้แต่ชื่อจริง จนกระทั่งพวกเขาถูกเปิดเผยให้ทราบโดยตำรวจที่จับกุม ทั้งหมดถูกจับที่บ้านของพวกเขาเอง และถูกตั้งข้อหาว่าสมคบกันกระทำความผิดตาม มาตรา 3 ของ CMA 1990 และข้อหาใช้บริการของ British Telecom โดยทุจริต 2 ใน 3 คนนี้ได้รับการเปิดเผยว่าคือ Woods และ Strickland โดย Woods ยอมรับว่าเขาเป็นสาเหตุให้เกิดความเสียหาย 15,000 ปอนด์ในระบบของ The Polytechnic of Central London และการกระทำของ Strickland ยังรวมถึงการ hack เข้าสู่ระบบเครือข่ายของ NASA และ ITN's Oracle พวกเขาถูกตัดสินลงโทษจำคุกคนละ 6 เดือน โดยศาล Southwark Crown Court เมื่อวันที่ 21 พฤษภาคม 1993

ผู้พิพากษา Michael Harris กล่าวว่า "เขาต้องการลงโทษจำคุกสำหรับการกระทำของจำเลย ทั้งนี้ เพื่อลงโทษสำหรับสิ่งที่จำเลยได้กระทำ และสำหรับความสูญเสียที่เกิดขึ้น และเพื่อยับยั้งผู้อื่นที่อาจจะพยายามกระทำความผิดเช่นนี้ เพราะอาจมีบางคนคิดว่า hacking คือสิ่งที่ไม่มีภัย แต่แท้จริงแล้วเป็นภัยอย่างยิ่งเพราะปัจจุบันคอมพิวเตอร์เป็นศูนย์กลางในชีวิตของพวกเรา มันบรรจุข้อมูลส่วนตัว ข้อมูลทางการเงิน ความลับของบริษัทและรัฐบาล รวมทั้งองค์กรเอกชนจำนวนมาก การให้บริการเหล่านี้ อาจเป็นการให้บริการในเรื่องเร่งด่วนขึ้นอยู่กับคอมพิวเตอร์ของพวกเขาที่จะให้บริการ จึงเป็นเรื่องสำคัญยิ่งที่คอมพิวเตอร์จะต้องอยู่ในสภาพที่สมบูรณ์ ต้องได้รับการปกป้อง การ hacking คือ การทำให้สภาพที่สมบูรณ์ต้องตกอยู่ในอันตราย

ดังนั้น hacker จำเป็นต้องได้รับการเตือนอย่างชัดแจ้งจากศาลว่า การกระทำของพวกเขาไม่อาจถูกยินยอมให้กระทำได้"[47]

จากคำตัดสินของศาลหลายคดีส่งผลให้กระแสต่อต้าน hacker เริ่มตื่นตัวขึ้น ทำให้หนังสือเล่มหนึ่งที่ชื่อ "hacker's Handbooks (2)" ถูกถอนออกจากการพิมพ์เนื่องจากความกลัวว่าเนื้อหาของหนังสือที่เกี่ยวข้องกับการ hack จะทำให้เป็นความผิดฐานแนะนำหรือร่วมกันกับผู้อื่นในการกระทำความผิด

แม้ CMA จะมีบทบัญญัติที่เอาผิดกับผู้ก่ออาชญากรรมทางคอมพิวเตอร์ก็ตาม แต่ในปี ค.ศ.1992 กระทรวงการค้าและอุตสาหกรรม (The Department of Trade and Industry) ได้ตีพิมพ์รายงานเกี่ยวกับการใช้คอมพิวเตอร์โดยมิชอบ รายงานเปิดเผยว่าบริษัทใหญ่ๆ หลายแห่งเชื่อว่าพวกเขาจะไม่ได้ประโยชน์อะไรจากการฟ้องร้องดำเนินคดีภายใต้ CMA 1990 และพวกเขาไม่เต็มใจที่จะรายงานถึงอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นต่อเจ้าพนักงานตำรวจ เนื่องจากคดีดังกล่าวมิใช่คดีทางแพ่ง ไม่มีเรื่องการคืนทรัพย์หรือชดใช้ค่าเสียหาย ดังนั้น พวกเขาจะไม่ได้รับประโยชน์โดยตรง ด้วยเหตุนี้จึงมีคดีจำนวนน้อยที่ขึ้นสู่ศาล การแก้ไขอาจกระทำได้โดยใช้บริษัทประกัน โดยให้บริษัทประกันกดดันบริษัทผู้เสียหายให้เข้าแจ้งความเรื่องที่เกิดขึ้น อย่างไรก็ตาม การกระตุ้นให้บริษัทผู้ได้รับความเสียหายกล้าเข้าแจ้งความหรือรายงานความเสียหายให้เจ้าพนักงานตำรวจทราบนั้น ขึ้นอยู่กับความมีประสิทธิภาพของเจ้าพนักงานตำรวจในการจัดการกับอาชญากรรมทางคอมพิวเตอร์ เพราะกลุ่มผู้ประกอบธุรกิจยังมีข้อสงสัยและได้แสดงความห่วงใยว่า เจ้าพนักงานตำรวจมีทักษะความรู้ด้านคอมพิวเตอร์มากน้อยเพียงใดในการที่จะสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์ อุปสรรคสำคัญอยู่ที่การดำเนินคดีกับผู้กระทำผิด แม้ว่าจะมีหน่วยงานพิเศษเพื่อสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ คือ The Computer Crime Unit in the Metropolitan Police แต่เนื่องจากการแจ้งความในปริมาณน้อย ส่งผลให้เจ้าพนักงานตำรวจไม่มีโอกาสที่จะฝึกฝนการสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์ในรูปแบบต่างๆ ได้อย่างมีประสิทธิภาพ[48]

---

[47] ข้อมูลดังกล่าวแปลมาจาก Computer Misuse and Computer Law , ใน Http://www.comp.glam.ac.uk/ism23/ additional-material/ computer-crime-&-law.html , (3 November 2000).

[48] Ibid.

3. Consumer Credit Act of 1974

การทุจริตต่อบัตรเครดิตเกิดขึ้นด้วยวิธีการหลากหลายรูปแบบ ส่งผลให้ผู้ถือบัตรที่แท้จริงต้องแบกรับภาระในการชำระเงินค่าสินค้าและบริการให้แก่ธนาคารหรือสถาบันผู้ออกบัตร ทั้งที่ตนมิได้เป็นผู้ก่อหนี้สินดังกล่าวให้เกิดขึ้น อย่างไรก็ตาม เมื่อพิจารณาถึง Consumer Credit Act of 1974 ซึ่งเป็นกฎหมายคุ้มครองผู้บริโภคของประเทศอังกฤษแล้ว จะเห็นว่าแม้กฎหมายดังกล่าวจะถูกบัญญัติขึ้นมาตั้งแต่ปี ค.ศ.1974 แต่โดยเนื้อหาสาระของกฎหมายฉบับนี้ยังสามารถให้ความคุ้มครองและเยียวยาความเสียหายต่อเจ้าของบัตรที่แท้จริงซึ่งถูกคนร้ายนำบัตรของตนไปใช้โดยปราศจากอำนาจ

ในมาตรา 83-84 ของ Consumer Credit Act ได้บัญญัติควบคุมถึงความรับผิดสำหรับการใช้บัตรเครดิตโดยปราศจากอำนาจ มาตรา 83 (1) ได้วางหลักการโดยทั่วไปว่า "ลูกหนี้ภายใต้ข้อตกลงที่ถูกบัญญัติจะไม่มีความรับผิดชอบต่อเจ้าหนี้จากการสูญเสียใดๆ ซึ่งเกิดจากการใช้ประโยชน์จากเครดิตโดยบุคคลอื่นไม่ว่าโดยตรงหรือเป็นตัวแทนของลูกหนี้" ดังนั้น หากสัญญาระหว่างผู้ออกบัตรและผู้ถือบัตรไม่ได้ก่อให้เกิดข้อกำหนดใดๆ เกี่ยวกับการใช้บัตรเครดิตโดยทุจริต เจ้าของบัตรจึงไม่ต้องรับผิดชอบถ้ามีการใช้บัตรนั้นโดยทุจริต อย่างไรก็ตาม มาตรา 84 ได้กำหนดข้อยกเว้นของหลักทั่วไปในมาตรา 83 (1) โดยกำหนดว่า "มาตรา 83 ไม่ได้ป้องกันลูกหนี้ภายใต้ข้อตกลงหลักฐานแห่งสินเชื่อจากการทำให้ถูกรับผิดชอบในการขยายความรับผิดชอบขั้นสูงถึง 50 ปอนด์ (หรือเท่ากับวงเงินถ้าน้อยกว่า 50 ปอนด์) สำหรับการสูญเสียต่อเจ้าหนี้ ซึ่งเกิดจากการใช้หลักฐานแห่งสินเชื่อนั้นๆ โดยบุคคลอื่นในระหว่างระยะเวลาซึ่งเริ่มต้นจากเมื่อหลักฐานแห่งสินเชื่อนั้นยกเว้นการถูกครอบครองของบุคคลที่มีอำนาจใดๆ และถึงแม้เมื่อหลักฐานแห่งสินเชื่อนั้นถูกครอบครองอีกครั้งหนึ่งจากผู้มีอำนาจ"[49]

<u>ความรับผิดของลูกหนี้</u> [50]

---

[49] จนิษฐ คันธสมบูรณ์, "การทุจริตโดยใช้บัตรเครดิต," (วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย , 2538), หน้า 73.

[50] Robert Lowe and Geoffrey Woodroffe , <u>Consumer Law and Practice</u> , (London : Publish by Sweet & Maxwell Ltd , 1985) , p.339-340.

ภายใต้เงื่อนไขข้อตกลงหรือสัญญาบัตรเครดิต ลูกหนี้ไม่ต้องรับผิดจากการที่ผู้อื่นนำบัตรเครดิตของตนไปใช้โดยปราศจากอำนาจ เว้นแต่ลูกหนี้ยอมรับการนำบัตรนั้นไปใช้อยู่ก่อนแล้ว หรือการใช้บัตรนั้นได้ถูกยอมรับโดยลูกหนี้

หลักในมาตรา 84 ของ Consumer Credit Act ได้กำหนดถึงกรณีที่ผู้อื่นนำบัตรเครดิตไปใช้โดยปราศจากอำนาจ ดังนี้

1. ลูกหนี้ต้องมีหนังสือบอกกล่าวเรื่องบัตรสูญหายหรือถูกนำไปใช้โดยมิชอบทันทีที่สามารถทำได้ ทั้งนี้ ภายในข้อตกลงหรือสัญญาบัตรเครดิตต้องระบุรายละเอียดเกี่ยวกับชื่อ ที่อยู่ และหมายเลขโทรศัพท์ของผู้ที่หนังสือบอกกล่าวจะถูกส่งไปถึง หากไม่มีรายละเอียดของข้อตกลงในส่วนนี้ ลูกหนี้จะไม่ต้องรับผิดสำหรับค่าใช้จ่ายที่เกิดขึ้นทั้งหมดจากการที่บัตรถูกนำไปใช้โดยปราศจากอำนาจ

2. ลูกหนี้ไม่ต้องรับผิดสำหรับความเสียหายที่เกิดเพิ่มขึ้นภายหลังที่เจ้าหนี้ได้รับการบอกกล่าวถึงบัตรสูญหายหรือถูกขโมยหรือเหตุอื่น ไม่ว่าด้วยวาจากหรือเป็นลายลักษณ์อักษร แต่หากเป็นการบอกกล่าวด้วยวาจาจะถือว่ามีผลต่อเมื่อเจ้าหนี้ได้รับการบอกกล่าวเป็นลายลักษณ์อักษรตามมาภายใน 7 วัน

3. ความรับผิดของผู้ถือบัตรขึ้นอยู่บุคคลผู้ซึ่งนำบัตรนั้นไปใช้โดยปราศจากอำนาจ หากบัตรถูกใช้โดยผู้ซึ่งได้รับบัตรมาไว้ในครอบครองโดยความยินยอมของลูกหนี้ ลูกหนี้ต้องรับผิดโดยไม่จำกัดจำนวน ส่วนกรณีอื่นความรับผิดของลูกหนี้ถูกจำกัดในวงเงิน 50 ปอนด์ หรือเท่ากับวงเงินหากน้อยกว่า 50 ปอนด์

บทบัญญัติของกฎหมายดังกล่าวได้กำหนดความรับผิดของผู้ถือบัตรสำหรับความเสียหายที่เกิดขึ้นจากการที่บุคคลอื่นนำบัตรเครดิตของตนไปใช้โดยปราศจากอำนาจ และปราศจากความรับรู้ของผู้ถือบัตรที่แท้จริง โดยผู้ถือบัตรถูกจำกัดให้ต้องรับผิดชอบสำหรับค่าใช้จ่ายที่เกิดขึ้นในวงเงินไม่เกิน 50 ปอนด์สำหรับความเสียหายที่เกิดจากการใช้บัตรเครดิตโดยปราศจากอำนาจในแต่ละครั้ง ซึ่งเจตนารมณ์และบทบัญญัติของกฎหมายนี้มิได้มุ่งเน้นหรือจำกัดว่าความเสียหายที่เกิดขึ้นจะต้องเกิดจากการทุจริตต่อบัตรเครดิตในลักษณะใด ดังนั้น ความ

รับผิดของผู้ถือบัตรที่แท้จริงจึงควรถูกจำกัดไว้สำหรับการทำธุรกรรมทุกประเภท รวมถึงการใช้มายเลขบัตรเครดิตของผู้อื่นโดยปราศจากอำนาจเพื่อการสั่งซื้อสินค้าหรือบริการบนอินเตอร์เนทด้วย[51]

อย่างไรก็ตาม ดังที่กล่าวไว้แล้วในตอนต้นว่า การที่คนร้ายนำบัตรเครดิตของผู้อื่นไปใช้โดยปราศจากอำนาจบนอินเตอร์เนทนั้น คนร้ายอาจครอบครองทั้งหมายเลขบัตรและตัวบัตรด้วยเนื่องจากการขโมยหรือการสูญหาย ซึ่งหากกรณีเป็นเช่นนี้ ผู้ถือบัตรย่อมสามารถที่จะมีหนังสือบอกกล่าวไปยังเจ้าหนี้ได้เมื่อตรวจพบความสูญหาย แต่หากเป็นกรณีที่ตัวบัตรยังคงอยู่ในความครอบครองของผู้ถือบัตร แต่คนร้ายได้หมายเลขบัตรเครดิตไปอันเนื่องมาจากการเจาะระบบและขโมยข้อมูลบนระบบเครือข่าย กรณีนี้ผู้ถือบัตรย่อมไม่มีทางที่จะมีหนังสือแจ้งถึงความสูญหายของบัตรไปยังเจ้าหนี้ได้ เพราะตนยังคงครอบครองบัตรนั้นอยู่และไม่ทราบว่ามีผู้ใดกำลังใช้เฉพาะหมายเลขบัตรเครดิตของตนโดยปราศจากอำนาจ ผู้ถือบัตรจะมีหนังสือบอกกล่าวไปยังเจ้าหนี้ได้ก็ต่อเมื่อการใช้บัตรโดยปราศจากอำนาจได้เกิดขึ้นแล้ว ซึ่งกรณีนี้ผู้ถือบัตรต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นในวงเงินไม่เกิน 50 ปอนด์

จากปัญหาการทุจริตต่อบัตรเครดิตบนอินเตอร์เนทที่เกิดขึ้น โดยการที่คนร้ายใช้เพียงหมายเลขบัตรเครดิตนั้น มีข้อที่น่าคิดว่าการใช้บัตรเครดิตในลักษณะนี้ บัตรสามารถถูกใช้โดยที่ผู้ถือบัตรและร้านค้าไม่ได้พบปะเห็นหน้ากัน ไม่มีหลักฐานใดให้ลงชื่อ ลูกค้าจะให้ข้อมูลที่ปรากฏบนบัตรแก่ร้านค้า เช่น หมายเลขบัตร วันหมดอายุ ชื่อผู้ถือบัตร เป็นต้น ข้อมูลที่ลูกค้าแจ้งไปยังร้านค้านั้นมิได้แสดงให้เห็นว่าลูกค้าคนนั้นเป็นผู้ครอบครองบัตรหรือเป็นเจ้าของบัตรที่แท้จริง อาจเป็นไปได้ว่าลูกค้ารายนั้นเป็นผู้ที่ทราบหมายเลขบัตรจากการที่บัตรเคยผ่านมือ หรือได้ข้อมูลมาจากการลักลอบสกัดหรือดักฟัง (Intercept) จุดประสงค์ของการซื้อขายก็เพื่อให้ร้านค้าส่งสินค้าไปให้ ดังนั้น ร้านค้าควรตรวจสอบที่อยู่ของผู้ถือบัตรผ่านทางธนาคาร ว่าสถานที่ที่ลูกค้าแจ้งความประสงค์ให้ส่งสินค้าไปให้นั้นเป็นสถานที่นอกเหนือจากที่ผู้ถือบัตรระบุไว้กับธนาคารหรือไม่ เพื่อร้านค้าอาจปฏิเสธการซื้อขายรายนั้นได้ แต่อาจเกิดปัญหากับกรณีที่ลูกค้าแจ้งให้จัดส่งสินค้าไปยังสถานที่ของบุคคลที่สามซึ่งจะยากแก่การตรวจสอบ ภาระหน้าที่ของบริษัทผู้ออกบัตรคงมีแค่เพียงการตรวจสอบในเบื้องต้นว่าผู้ถือบัตรเคยแจ้งเรื่องบัตรสูญหายหรือถูกขโมยไว้หรือไม่ รวมถึงการตรวจสอบวงเงินบัตรเครดิตเท่านั้น ผู้ออกบัตรมิได้ถูกกำหนดให้ต้องตรวจสอบว่าลูกค้าที่กำลังทำการซื้อขายกับร้านค้าบนอินเตอร์เนทนั้นเป็นผู้มีอำนาจใช้บัตรหรือไม่ ภาระความรับผิดที่จะเกิดขึ้น

---

[51] ข้อมูลดังกล่าวแปลมาจาก UK.Consumer Rights ใน Http://www.workz.com/content/396.asp,(12 July 2001).

กับการทุจริตต่อบัตรเครดิตบนอินเตอร์เนทไม่ควรจะตกอยู่กับเจ้าของบัตรที่แท้จริงหรือบริษัทผู้ออกบัตร เนื่องจากแนวคิดที่ว่าผู้ที่ได้รับผลประโยชน์จำนวนมหาศาลอันเนื่องมาจากความสะดวกสบายของพาณิชย์อิเล็คทรอนิคส์นั้นก็คือร้านค้า นั่นเอง ดังนั้น ภาระความเสี่ยงจึงควรถูกผลักให้เป็นของร้านค้าหากมีการทุจริตเกิดขึ้น หากผู้ถือบัตรปฏิเสธว่ามิได้เป็นผู้ให้ข้อมูลบัตรแก่ร้านค้าในการทำธุรกรรมนั้น ไม่หลักฐานการส่งสินค้าให้แก่ผู้ถือบัตร หรือหลักฐานใดที่ผู้ถือบัตรลงชื่อไว้ ธนาคารก็ไม่อาจเรียกเก็บเงินค่าใช้จ่ายนั้นจากบัญชีของผู้ถือบัตรได้ เพราะเพียงแต่การใช้ข้อมูลบัตรไม่สามารถระบุได้ว่าผู้ถือบัตรเป็นผู้ทำธุรกรรมนั้น[52]

ด้วยเหตุนี้ จึงมีการแก้ไขปรับปรุงกฎหมาย Consumer Credit Law ซึ่งผ่านการอนุมัติจากสภาของอังกฤษแล้วเมื่อวันที่ 13 มีนาคม 2001 และจะมีผลบังคับใช้ในวันที่ 1 มกราคม 2002 หลักสำคัญของกฎหมายฉบับนี้มิใช่เพื่อต้องการลงโทษผู้กระทำผิด แต่ต้องการให้ความคุ้มครองผู้บริโภคเป็นหลัก โดยผู้ถือบัตรที่ถูก Hacker หรือผู้อื่นขโมยหมายเลขบัตรเครดิตโดยปราศจากตัวบัตร จะไม่ต้องรับผิดต่อความเสียหายใดที่เกิดขึ้น แต่หากเป็นกรณีที่ตัวบัตรเครดิตนั้นสูญหายไปด้วย ผู้ถือบัตรมีหน้าที่ต้องแจ้งถึงการสูญหายหรือถูกขโมยเป็นลายลักษณ์อักษรไปยังเจ้าหนี้ และต้องพิสูจน์ด้วยว่าบัตรนั้นมิได้สูญหายอันเนื่องมาจากความประมาทของผู้ถือบัตร ซึ่งจะทำให้ผู้ถือบัตรถูกจำกัดความรับผิดสูงสุดไว้ในวงเงินไม่เกิน 100 ปอนด์[53]

เทคโนโลยีรักษาความปลอดภัยของข้อมูลบนอินเตอร์เนท

แม้ปัจจุบันการทำธุรกิจผ่านเครือข่ายอินเตอร์เนทจะเพิ่มจำนวนมากขึ้น แต่อย่างไรก็ตามยังมีผู้ใช้บริการอีกจำนวนมากยังลังเลที่จะซื้อขายสินค้าหรือทำธุรกรรมต่างๆ ผ่านเครือข่ายอินเตอร์เนท ทั้งนี้ เนื่องจากความไม่มั่นใจในระบบรักษาความปลอดภัยของข้อมูลบนเครือข่าย

---

[52] ข้อมูลดังกล่าวแปลมาจาก Electronic Commerce : Who carries the risk of fraud? ใน Http://clj.warwick.ac. uk/jilt/ 00-3/bohm.html, (3 November 2000).

[53] ข้อมูลดังกล่าวแปลมาจาก Internet opens new horizons for credit card fraud ใน Http://www.cyprus-mail.com/june/ 3/feature8.htm, (3 November 2000).

ดังกล่าว ในทุกวันนี้มีการแพร่กระจายของการจารกรรมข้อมูลผ่านระบบคอมพิวเตอร์เป็นอย่างมากโดยกลุ่มนักขโมยข้อมูล (Hacker) ดังนั้น สิ่งสำคัญที่จะเข้ามาช่วยสร้างความมั่นใจให้แก่ผู้ใช้บริการอินเตอร์เนทก็คือเทคโนโลยีรักษาความปลอดภัยของข้อมูล

1. จุดประสงค์ของระบบรักษาความปลอดภัย[54]

1. เพื่อรักษาความลับของข้อมูล (Confidentiality)

หมายถึง การปกป้องข้อมูลไม่ให้ถูกเปิดเผยต่อบุคคลอื่นที่ไม่ได้รับอนุญาตอย่างถูกต้องและหากมีการขโมยข้อมูลไปแล้วก็จะไม่สามารถอ่านหรือทำความเข้าใจข้อมูลนั้นได้เนื่องจากมีวิธีรักษาความปลอดภัยของข้อมูลอย่างเพียงพอ

2. เพื่อป้องกันและปลอมแปลงข้อมูล (Integrity)

หมายถึง การรักษาความถูกต้องของข้อมูลและป้องกันไม่ให้มีการเปลี่ยนแปลงแก้ไขข้อมูลโดยมิได้รับอนุญาต ซึ่งจะต้องมีระบบควบคุมว่าผู้ใดจะสามารถเข้าถึงข้อมูลได้และหากเข้าถึงข้อมูลได้แล้วจะสามารถทำอะไรกับข้อมูลนั้นๆ ได้บ้าง เช่น การอ่านหรือเขียนข้อมูลได้เพียงอย่างเดียว หรือสามารถทำได้ทั้งการอ่านและเขียนข้อมูลนั้น

3. เพื่อทำให้ระบบนั้นสามารถทำงานได้ตามปกติและเต็มประสิทธิภาพ (Availability)

หมายถึง ระบบจะต้องสามารถทำงานได้ตามความมุ่งหมายในการใช้ และต้องมีขีดความสามารถ ปฏิบัติงานได้ในปริมาณและเวลาที่กำหนด

2. การเข้ารหัสและถอดรหัสข้อมูล (Encryption and Decryption)

จากเหตุการณ์ที่ Mexus เข้าถึงข้อมูลของลูกค้าบริษัท ซีดียูนิเวิร์สและครอบครอบข้อมูลเกี่ยวกับหมายเลขบัตรเครดิตของลูกค้าของบริษัทกว่า 300,000 ราย ดังที่กล่าวไว้แล้วในบทที่ 2 นั้น หลังเกิดเหตุบริษัท ซีดียูนิเวิร์ส ได้โยนความผิดของเรื่องทั้งหมดให้กับซอฟท์แวร์ที่ซื่อ

---

[54] ณรงค์ชัย นิมิตรบุญอนันต์ , Computer Security for E-Commerce , (กรุงเทพมหานคร : SUM Publishing Department, 2542) , หน้า 6-7.

ไอซีเวอริไฟ (IC Verify) ซึ่งผู้เชี่ยวชาญให้ความเห็นว่าซอฟท์แวร์ที่บริษัทใช้ในการออกแบบระบบการซื้อขายดังกล่าวนี้มีการเก็บข้อมูลเกี่ยวกับบัตรเครดิตไว้ในรูปแบบตัวอักษรธรรมดา (Text File) โดยไม่มีการเข้ารหัส (Encrypt) ไว้ ทำให้ผู้ที่ได้ข้อมูลนี้ไปสามารถนำไปใช้ได้ทันที เหตุการณ์ดังกล่าวทำให้ผู้ขายสินค้าหรือบริการผ่านอินเตอร์เนทหันมาคำนึงถึงเทคโนโลยีการเข้ารหัสเพื่อสร้างความมั่นใจให้ลูกค้าผู้มาซื้อสินค้าว่า ข้อมูลส่วนตัวของลูกค้าจะไม่ถูกอาชญากรขโมยไปใช้อีก

การเข้ารหัสและถอดรหัสข้อมูล (Encryption and Decryption) เป็นวิธีการหนึ่งที่นำมาใช้เพื่อสร้างความปลอดภัยให้แก่ข้อมูลที่ส่งผ่านระบบคอมพิวเตอร์ จุดประสงค์ของการเข้ารหัสข้อมูล ก็เพื่อรักษาความลับของข้อมูลโดยที่ข้อมูลนั้นจะถูกเปิดเผยต่อบุคคลที่ได้รับอนุญาตเท่านั้น กระบวนการนี้เรียกอีกอย่างหนึ่งว่า Cryptography หมายถึงศาสตร์การรักษาความลับของข้อมูล

การเข้ารหัส คือ การทำให้ข้อความที่ต้องการส่งผ่านระบบเครือข่ายคอมพิวเตอร์ที่เป็นข้อความที่สามารถอ่านได้ (Clear Text) ซึ่งหากมีการขโมยข้อมูลในระหว่างทำการส่งแล้ว จะเกิดความเสียหายเนื่องจากการเปิดเผยข้อมูลที่เป็นความลับ ดังนั้น วิธีป้องกันก็คือการทำให้ข้อมูลที่เป็นความลับนั้นเป็นข้อความที่ไม่สามารถอ่านออกได้ (Cipher Text) จากนั้นจึงส่งข้อมูลที่ไม่สามารถอ่านได้นี้ไปยังจุดหมายปลายทางบนระบบเครือข่ายต่อไป ซึ่งหากในระหว่างการส่งนั้นมีการขโมยข้อมูลไปโดยผู้ไม่ประสงค์ดี ข้อมูลนั้นก็จะไม่เปิดเผยความลับแก่บุคคลนั้นเนื่องจากบุคคลดังกล่าวจะไม่สามารถอ่านและเข้าใจข้อความนั้นได้ เพราะในการอ่านข้อความ Cipher Text ได้นั้นจะต้องอาศัยการถอดรหัส (Decryption) อีกขั้นตอนหนึ่ง

การถอดรหัส (Decryption) คือ การเปลี่ยนข้อความที่ไม่สามารถอ่านออกได้ (Cipher Text) ให้กลับเป็นข้อความที่สามารถอ่านออกได้ (Clear Text) โดยการใช้กุญแจถอดรหัส (Decryption Key) ดังนั้น ผู้ใดก็ตามที่จะสามารถอ่านข้อความที่ได้รับมาได้จะต้องมีกุญแจถอดรหัส ซึ่งหากกุญแจเข้ารหัสและถอดรหัสเหมือนกันทั้งสองข้างจะเรียกกระบวนการนี้ว่า Symmetric Key Encryption แต่หากกุญแจเข้ารหัสและถอดรหัสไม่จำเป็นต้องเหมือนกันทั้งสองข้างจะเรียกกระบวนการนี้ว่า Asymmetric Key Encryption

การเข้ารหัสเป็นเครื่องมือในการรักษาความปลอดภัยของข้อมูลในการพาณิชย์อิเล็คทรอนิคส์ การเข้ารหัสและการถอดรหัสจะทำโดยการใช้รหัสซึ่งรู้กันระหว่างฝ่ายผู้ที่ทำการติดต่อกันเท่านั้น ซึ่งทำให้ผู้ที่ติดต่อกันนั้นมั่นใจได้ว่าไม่มีใครสามารถแอบอ่านข้อมูลได้ ในเบื้องต้น

การเข้ารหัสเป็นไปแบบง่ายๆ ที่เรียกว่าการเข้ารหัสแบบ Secret Key โดยผู้รับและผู้ส่งจะถือกุญแจรหัสดอกเดียวกัน โดยผู้ส่งจะใช้กุญแจรหัสเพื่อเข้ารหัสข้อมูลก่อนส่ง และผู้รับจะต้องใช้กุญแจรหัสที่มีรูปแบบเดียวกันกับที่ผู้ส่งถืออยู่สำหรับถอดรหัสข้อมูล ซึ่งต่อมาการเข้ารหัสวิธีนี้ไม่ได้รับความนิยม เนื่องจากผู้รับและผู้ส่งต้องแลกเปลี่ยนรหัสลับกันก่อนเพื่อใช้ตรวจสอบความถูกต้อง ซึ่งในระหว่างนั้นอาจทำให้รหัสถูกขโมยหรือถูกลักลอบนำไปใช้ นอกจากนี้การประกอบการพาณิชย์อิเล็คทรอนิคส์ส่วนใหญ่จะทำกับบุคคลที่ไม่เคยรู้จักกันมาก่อน จึงเป็นการยากและไม่ปลอดภัยที่จะให้รหัสลับซึ่งกันและกัน จึงได้มีการพัฒนาเทคนิคการเข้ารหัสเป็นแบบ Public key โดยการเข้าและถอดรหัสที่แตกต่างกันประกอบด้วยกุญแจสาธารณะ (Public key) ที่เป็นที่ทราบทั่วไปต่อสาธารณชนและอีกรหัสหนึ่งคือกุญแจลับ (Private key) ที่ผู้เป็นเจ้าของเท่านั้นเป็นผู้เก็บรักษาไว้ การเข้ารหัสแบบนี้ไม่จำต้องมีการแลกเปลี่ยนกุญแจลับกันแต่อย่างใด ซึ่งถือเป็นพื้นฐานของการประกอบการพาณิชย์อิเล็คทรอนิคส์[55]

3. **ระบบรักษาความปลอดภัยของข้อมูล**

ด้วยเหตุที่การซื้อขายผ่านระบบอินเตอร์เนทหรือ E-Commerce นับวันจะเติบโตขึ้นเรื่อยๆ อย่างไม่หยุดยั้ง ในอนาคตอันใกล้นี้การจับจ่ายใช้สอยในหลายๆ ด้าน อาทิ การจ่ายค่าบริการต่างๆ ไม่ว่าจะเป็นค่าไฟฟ้า ค่าน้ำประปา ค่าโทรศัพท์ ฯลฯ หรือการจ่ายค่าประกันต่างๆ การฝาก ถอน โอนเงินจากบัญชีในธนาคารก็จะสามารถทำได้อย่างสะดวกสบายจากคอมพิวเตอร์ที่เชื่อมเข้าสู่ระบบอินเตอร์เนทภายในบ้านของทุกคน แต่การที่จะกระทำเช่นนี้ได้จะต้องมีระบบการแลกเปลี่ยนข้อมูลข่าวสารผ่านระบบเครือข่ายคอมพิวเตอร์ที่มีความปลอดภัยสูงมากพอที่จะใช้เป็นสื่อในการส่งข้อมูลทางด้านการเงินได้ อีกทั้งยังต้องมีความง่ายและความคล่องตัวในการนำไปใช้กับทุกๆ ฝ่ายที่เกี่ยวข้อง ไม่ว่าจะเป็นธนาคาร สถาบันการเงิน ผู้ค้า หรือบริษัทห้างร้านต่างๆ รวมทั้งผู้จับจ่ายใช้สอยด้วย ดังนั้น บริษัท Visa Card และบริษัท Master Card ซึ่งเป็นบริษัทผู้ให้บริการบัตรเครดิตรายใหญ่จึงได้คิดค้นระบบรักษาความปลอดภัยในการซื้อขายผ่านอินเตอร์เนทและตั้งเป็นมาตรฐานกลางร่วมกัน โดยใช้ชื่อว่า SET หรือ Secure Electronics Transactions ซึ่งแน่นอนว่ามาตรฐานของ SET นั้น ต้องอิงอยู่กับการใช้บัตรเครดิตของบริษัทดังกล่าวซึ่งเป็นผู้พัฒนาระบบ

---

[55] กฤษณะ ช่างกล่อม , กฎหมายลายมือชื่อดิจิตอล , (กรุงเทพมหานคร: โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ, 2542) , หน้า 17-18.

4. **ระบบ** SET (Secure Electronics Transactions)

ระบบ SET หรือ Secure Electronics Transactions นั้น เป็นระบบที่ใช้ในการจับจ่ายใช้สอยเงินโดยใช้บัตรเครดิตเป็นสื่อผ่านระบบเครือข่ายคอมพิวเตอร์ และเป็นระบบที่ได้รับการพัฒนาขึ้นมาโดยความร่วมมือกันระหว่างบริษัท Visa Card และบริษัท Master Card การที่บริษัทยักษ์ใหญ่ทั้งสองบริษัทกำหนดมาตรฐานของระบบการจับจ่ายใช้สอยที่เรียกว่า SET ขึ้นมานั้น มีผลกระทบอย่างมากมายมหาศาลต่อวงการธุรกิจในระดับโลกที่เกี่ยวข้องกับการใช้บัตรต่างๆ เป็นสื่อในการจ่ายเงินแทนเงินสดไม่ว่าจะเป็นบัตรเครดิต บัตรเงินสด บัตรสมาร์ทการ์ด หรือบัตรชนิดอื่นๆ ทั้งนี้เหตุผลประการสำคัญที่มาตรฐาน SET นี้จะมีผลกระทบสำคัญต่อวงการนี้คือ บริษัททั้งสองครอบครองส่วนแบ่งในตลาดโลกไว้ทั้งสิ้นประมาณ 75% โดยที่บริษัท Visa Card มีส่วนแบ่ง 50% และบริษัท Master Card มีส่วนแบ่ง 25% โดยประมาณ ดังนั้น ธนาคารและสถาบันการเงินต่างๆ ที่ต้องการให้บริการทางการเงินแก่ลูกค้าของตนโดยใช้บัตรต่างๆ เป็นสื่อนั้น จะต้องหันมาพิจารณาอย่างจริงจังและเตรียมพร้อมไว้อย่างดี สำหรับระบบ SET ที่จะเข้ามามีบทบาทสำคัญยิ่งต่อมาตรฐานของสื่ออิเล็คทรอนิคส์ในระบบการเงินของโลก[56]

ในการทำธุรกิจพาณิชย์อิเล็คทรอนิคส์หรือ E-Commerce นี้จะประสบความสำเร็จได้ก็ต่อเมื่อผู้ใช้สื่ออิเล็คทรอนิคส์มีความมั่นใจว่าระบบและมาตรฐานการจ่ายเงินนั้นๆ จะสามารถเก็บรักษาความปลอดภัยของข้อมูลทางด้านการเงินได้เป็นอย่างดี เช่น หมายเลขบัตรเครดิตของผู้ซื้อ จะต้องได้รับการปกป้องไม่ให้รั่วไหลได้เลย SET เป็นมาตรฐานหรือข้อตกลงในการทำธุรกรรมบนอินเตอร์เนทที่มีความปลอดภัยระหว่างผู้ซื้อ ร้านค้า ธนาคารหรือสถาบันการเงิน โดยใช้เทคโนโลยีการเข้ารหัสข้อมูลด้วยวิธีการและวัตถุประสงค์ดังนี้

- เพื่อรักษาความลับของข้อมูล(Confidentiality) อันได้แก่ ข้อมูลหมายเลขบัตรเครดิตและที่อยู่ของลูกค้า เป็นต้น โดยใช้วิธีการเข้ารหัสข้อมูล (Encryption)
- เพื่อรักษาความถูกต้องของข้อมูล (Integrity) โดยเฉพาะจำนวนเงินที่ร้านค้าจะสามารถถอนและโอนจากจากบัญชีของลูกค้านั้นจะต้องไม่อาจเปลี่ยนแปลงแก้ไขได้โดยไม่ได้รับอนุญาต โดยการใช้ลายเซ็นดิจิตอลในการรับประกันความถูกต้อง

---

[56] ณรงค์ชัย นิมิตรบุญอนันต์ , Computer Security for E-Commerce , หน้า 206-207.

- เพื่อตรวจสอบและสามารถบ่งบอกชี้ชัดได้ว่าใครคือร้านค้าและลูกค้าผู้ถือบัตรที่เกี่ยวข้อง (Authentication) มิให้มีใครสามารถปลอมแปลงเข้ามาในระบบได้ โดยการใช้ลายเซ็นดิจิตอลและ Digital Certificate

5. **องค์ประกอบของ SET ประกอบด้วย**

1. ลูกค้าผู้ถือบัตรเครดิต (Cardholder) คือ ผู้ถือบัตรเครดิตที่ออกให้โดยธนาคารหรือบริษัทผู้ให้บริการ ซึ่งจะมีซอฟต์แวร์ประเภท Electronic Wallet ติดตั้งอยู่ในเครื่องคอมพิวเตอร์เพื่อสร้างกระบวนการในการรับส่งข้อมูล เช่น คำสั่งซื้อ, ข้อมูลการชำระเงิน ที่อยู่ภายใต้ Protocal ของ SET ระหว่างร้านค้า Payment Gateway และ CA โดยผู้ถือบัตรจะได้รับการรับรองทางอิเล็คทรอนิคส์ (Digital Certificate) ซึ่งการรับรองนั้นผู้ถือบัตรจะได้กุญแจเข้ารหัสทั่วไป (Public Key) ซึ่งจะมีอายุการใช้งานระยะเวลาหนึ่ง และกุญแจนี้ธนาคารจะลงลายมือชื่อทางอิเล็คทรอนิคส์ไว้ให้ด้วยเพื่อป้องกันการปลอมแปลง

2. ร้านค้า (Merchant) จะมี Server ที่คอยรับคำสั่งซื้อจากลูกค้า ตรวจสอบและยืนยันสถานภาพของผู้ซื้อจาก CA รวมทั้งทำหน้าที่ประมวลคำขออนุมัติการชำระเงินไปยัง Payment Gateway ร้านค้าจะได้รับการรับรองทางอิเล็คทรอนิคส์จากธนาคารด้วยเช่นกัน โดยจะได้รับกุญแจทั่วไป (Public Key) ของร้านค้าเองและของธนาคารด้วย

3. ธนาคารผู้จ่ายโอน (Processing Bank / Payment Gateway) ทำหน้าที่ตรวจสอบและอนุมัติการชำระเงินรวมทั้งการเรียกเก็บเงินจากลูกค้าผ่านเครือข่าย ผู้ที่ทำหน้าที่นี้ส่วนใหญ่จะเป็นธนาคารหรือสถาบันการเงินที่ทางร้านค้าเปิดบัญชีไว้ เพื่อรับสลิปใช้จ่ายจากลูกค้าบัตรเครดิต

4. Certification Authority (CA) ทำหน้าที่ออกใบรับรองหรือ Digital Certificate รวมถึงให้การรับรองสถานภาพของร้านค้า ลูกค้าผู้ถือบัตรและผู้ให้บริการ (Payment Gateway) เมื่อมีการร้องขอ ดูแลรับผิดชอบฐานข้อมูลของใบรับรอง เผยแพร่ข้อมูลสำคัญ เช่น ใบรับรองหมดอายุหรือถูกยกเลิก เป็นต้น ระบบ SET สามารถทำการพิสูจน์ผู้ซื้อและร้านค้าได้ว่าถูกต้อง ก่อนที่จะอนุญาตให้ทำการเบิกโอนเงินโดยผ่านระบบเครือข่ายคอมพิวเตอร์ โดยธนาคารจะสามารถรู้ว่าผู้ซื้อหรือผู้ถือบัตร (Cardholder) และร้านค้า (Merchant) นั้นเป็นผู้ที่ได้รับอนุญาตจากทางธนาคารจริงหรือไม่และได้ทำการติดต่อซื้อขายกันจริงหรือไม่ นอกจากนี้ยังสามารถเก็บ

ความลับระหว่างทั้งสามฝ่ายที่เกี่ยวข้องกับการซื้อขายนี้ได้ด้วย โดยที่ร้านค้าจะไม่มีทางรู้ข้อมูลเกี่ยวกับการเงินของลูกค้าได้เลย เช่น หมายเลขบัตรเครดิต หมายเลขบัญชี มีเพียงแต่ธนาคารที่เกี่ยวข้องเท่านั้นที่จะสามารถเข้ามาอ่านข้อมูลนี้ได้ ในขณะเดียวกันธนาคารผู้เบิกจ่ายก็ไม่อาจรู้รายละเอียดเกี่ยวกับสินค้าหรือการซื้อขายนั้นได้ เพียงแต่จะทำหน้าที่พิสูจน์และเบิกโอนเงินเท่านั้น

6. ขั้นตอนการใช้บัตรเครดิตบนอินเตอร์เนทผ่านระบบ SET[57]

1. ผู้ถือบัตร (Cardholder) สั่งซื้อสินค้าผ่านทางอินเตอร์เนทโดยใช้ Web Browser ซึ่งเป็นซอฟท์แวร์ที่ติดตั้งไว้กับเครื่องคอมพิวเตอร์เพื่อรับข้อมูลเกี่ยวกับการรับรองทางอิเล็คทรอนิคส์ (Digital Certificate) จากร้านค้าและทำการพิสูจน์ว่าเป็นร้านค้าที่ได้รับอนุญาตจริงหรือไม่ เมื่อพิสูจน์เสร็จสิ้นแล้วผู้ถือบัตรก็จะส่งใบสั่งซื้อผ่านเครือข่ายอินเตอร์เนทโดยใช้วิธีการเข้ารหัสข้อมูล (Encryption)

2. เมื่อร้านค้าได้รับคำสั่งซื้อแล้ว จะทำการพิสูจน์ทราบการรับรองทางอิเล็คทรอนิคส์ (Digital Certificate) ว่าเป็นผู้ซื้อที่ได้รับอนุญาตอย่างถูกต้องในระบบหรือไม่ จากนั้นจึงส่งข้อมูลต่อไปยังธนาคารที่เบิกจ่ายโดยใช้วิธีการเข้ารหัสข้อมูลเช่นกันเพื่อความปลอดภัยของข้อมูล

3. ธนาคารที่ทำการเบิกจ่าย (Processing Bank / Payment Gateway) จะพิสูจน์การซื้อขายนั้นจากฝ่ายผู้ถือบัตรและจากร้านค้า จากนั้นจึงตรวจสอบบัญชีของผู้ถือบัตรผ่านทางบริษัทเครดิตรวมถึงธนาคารหรือบริษัทผู้ออกบัตร

4. ธนาคารผู้จ่ายโอนจะทำการรับรองการจ่ายเงินและส่งไปยังร้านค้าโดยใช้วิธีการเข้ารหัสข้อมูลก่อนส่งข้อมูลออกไป

5. ร้านค้าจะส่งใบเสร็จรับเงินกลับไปยังผู้ถือบัตร

6. ธนาคารหรือบริษัทผู้ออกบัตรจะเรียกเก็บเงินจากผู้ถือบัตรโดยตรง

---

[57] เรื่องเดียวกัน , หน้า 209-210.

มาตรการตรวจสอบโดยร้านค้าบนอินเตอร์เนท

เดิมระบบบัตรเครดิตได้รับการออกแบบมาเพื่อใช้โดยต้องมีการแสดงตัวบัตรให้เห็นประกอบการทำธุรกรรมต่างๆ ด้วย เมื่อร้านค้าปฏิบัติตามกฎระเบียบของธนาคารหรือสถาบันผู้ให้บริการบัตรเครดิต (ผู้ออกบัตร) ร้านค้าก็จะได้รับการชำระเงินแม้ว่าบัตรเครดิตนั้นจะถูกขโมยมาก็ตาม ภาระความรับผิดชอบจะเปลี่ยนจากผู้ออกบัตรไปยังร้านค้า ในกรณีที่มีการชำระค่าสินค้าและบริการผ่านบัตรเครดิตโดยที่ร้านค้าไม่เห็นตัวบัตรที่แท้จริง เช่น การสั่งซื้อทางไปรษณีย์ โทรศัพท์ โทรสาร หรือทางอินเตอร์เนท โดยทั่วไปร้านค้าจะต้องรับผิดชอบต่อการชำระค่าสินค้าโดยบัตรเครดิตนั้น ถึงแม้ว่าธนาคารจะอนุมัติแล้ว แต่หากปรากฏในภายหลังว่าร้านค้าถูกโกงจากอาชญากรรมบัตรเครดิต ผู้ออกบัตรมักจะเพิ่มอัตราค่าบริการ โดยอ้างเหตุผลเรื่องความเสี่ยงที่สูงขึ้น ทั้งร้านค้ายังมีความเสี่ยงที่จะถูกปลดจากการเป็นคู่ค้ากับผู้ให้บริการบัตรเครดิตหากร้านค้าถูกโกงบ่อยครั้งเกินไป อาชญากรรมบัตรเครดิตไม่สามารถจะกำจัดให้หมดไปโดยสิ้นเชิง แต่จะต้องได้รับการจัดการ ร้านค้าจะต้องสร้างความสมดุลในการป้องกันอาชญากรรม โดยที่ไม่สร้างความไม่สะดวกกับลูกค้ามากเกินไป

ผู้ใช้บริการบนอินเตอร์เนทส่วนใหญ่มีความกังวลมากเกี่ยวกับความเป็นส่วนตัวและความปลอดภัยในการใช้บัตรเครดิตบนอินเตอร์เนท การรู้สึกว่ามีความเสี่ยงที่จะเกิดอาชญากรรมบัตรเครดิต ทำให้ร้านค้าออนไลน์นั้นไม่สามารถทำกำไรได้อย่างเต็มที่ เนื่องจากจำเป็นต้องจัดทำให้เว็บไซต์ของตนเองให้มีความปลอดภัยเพียงพอ อีกทั้งยังต้องมีนโยบายด้านความเป็นส่วนตัวในเว็บไซต์อีกด้วย ร้านค้าที่ให้บริการดาวน์โหลดซอฟต์แวร์ควรจะบังคับให้มีการให้ข้อมูลเพิ่มเติม เช่น ที่อยู่ที่สมบูรณ์ หมายเลขโทรศัพท์ และหมายเลขบัตรเครดิต 3-4 ตัว ร้านค้าต้องการข้อมูลเหล่านี้เพื่อที่จะสามารถตรวจสอบคำสั่งซื้อที่น่าสงสัยโดยบุคคล แทนที่จะใช้ระบบอัตโนมัติในการอนุมัติหรือปฏิเสธคำสั่งซื้อ การผสมผสานของวิธีการต่างๆ ดังต่อไปนี้เป็นวิธีการที่ดีที่สุดในการป้องกันการทุจริตต่อบัตรเครดิตบนอินเตอร์เนท[58]

1. **ระบบการตรวจสอบที่อยู่** (ADDRESS VERIFICATION SYSTEM / AVS)

---

[58] ข้อมูลดังกล่าวแปลมาจาก Merchant Credit Card Fraud ใน Http://www.wisco computing. com/articles/ ccfraud.htm (20 March 2002).

จากการสำรวจผู้ค้าที่เป็นสมาชิกของ Worldwide E-Commerce Fraud Prevention Network พบว่าวิธีที่ได้รับความนิยมและมีประสิทธิภาพมากที่สุดในการตรวจสอบอาชญากรรมคือ ระบบการตรวจสอบที่อยู่ AVS นั้นจะใช้เพียงรหัสไปรษณีย์และเลขที่ของที่อยู่ตามบัตรเครดิต เพราะแม้สินค้าจากคำสั่งซื้อจำนวนมากจะไม่ได้ถูกสั่งให้จัดส่งไปยังที่อยู่ตามบัตรก็ตาม แต่เจ้าของบัตรที่แท้จริงก็ควรที่จะรู้ที่อยู่ตามบัตร

2. **วิธีการตรวจสอบบัตร** (CARD VERIFICATION METHODS / CVM)

วิธีการตรวจสอบบัตร (VISA = CVV2, MasterCard = CvC2 และ American Express = CID) จะใช้รหัสตัวเลข 3-4 ตัวที่พิมพ์อยู่บนบัตร แต่ไม่ได้บันทึกลงในแถบแม่เหล็ก รหัสตัวเลขเหล่านี้จะไม่ปรากฏอยู่บนสลิปบัตรเครดิต ถ้าลูกค้าสามารถแจ้งหมายเลขนี้ได้ แสดงว่ามีบัตรอยู่ในมือจริง บัตรVisaบางส่วนยังไม่มีรหัส CVV2 (แต่จะมีในอนาคต) อาชญากรรมส่วนใหญ่จะเกิดจากการขโมยหมายเลขบัตรมากกว่าการขโมยบัตรจริงๆ CVM เป็นวิธีที่มีประสิทธิภาพที่สุดที่จะลดจำนวนอาชญากรรมบัตรเครดิต ร้านค้าที่รับคำสั่งซื้อทางอินเตอร์เนท ไปรษณีย์ และโทรศัพท์ ต้องถามรหัสจากลูกค้าก่อนเพราะไม่ได้พบปะลูกค้าโดยตรง Mastercard วางแผนที่จะบังคับให้ร้านค้าถามข้อมูลนี้ตั้งแต่วันที่ 1 เมษายน 2001 ในขณะที่ Visa แจ้งว่าไม่ได้บังคับใช้กฎนี้บนอินเตอร์เนท อย่างไรก็ตาม Visa บังคับให้ธนาคารและผู้ดำเนินการบัตร ใช้รหัส CVV2 ในการขออนุมัติวงเงิน รัฐบาลอังกฤษเตรียมที่จะบังคับใช้กฎเรื่องรหัสตัวเลขนี้บนอินเตอร์เนท โดยเริ่มในปี 2004

3. **รหัสผ่าน** (Passwords)

สมาชิกบัตรVisa สามารถลงทะเบียนใช้บริการการตรวจสอบของVisaผ่านทางเว็บไซต์ของผู้ออกบัตรของตน รหัสผ่านส่วนตัวจะถูกใช้เป็นเหมือนลายเซ็นต์ดิจิตอลสำหรับการซื้อสินค้าผ่านเว็บไซต์ เมื่อผู้ถือบัตรซื้อสินค้ากับร้านค้าออนไลน์ที่เป็นสมาชิก ร้านค้าจะสามารถตรวจสอบว่าผู้ถือบัตรเป็นตัวจริงหรือไม่ ร้านค้าจะต้องติดตั้งซอฟต์แวร์ของVisaในการที่จะตรวจสอบผู้ถือบัตร ผู้ถือบัตรจะต้องใส่รหัสผ่าน หรือสอดบัตรVisaสมาร์ทการ์ดในเครื่องอ่าน และใส่รหัส (pin)

4. **แฟ้มข้อมูลประวัติไม่ดี**

วิธีนี้คือการเก็บข้อมูลของความพยายามก่ออาชญากรรม ได้แก่ ข้อมูลลูกค้าที่มี

ปัญหาบันทึกการไม่ชำระเงิน และลูกค้าที่ได้รับคืนเงิน แฟ้มข้อมูลนี้ควรจะบันทึกชื่อลูกค้า ที่อยู่บนบัตร สถานที่ส่งสินค้า หมายเลขโทรศัพท์ หมายเลขบัตรเครดิต IP และ e-mail address บันทึกจากร้านค้า โดยที่คำสั่งซื้อที่เข้ามาสามารถนำไปเทียบกับฐานข้อมูลที่มีอยู่ วิธีนี้สามารถป้องกันอาชญากรจากการทำผิดซ้ำๆ โดยที่มีค่าใช้จ่ายต่ำ แต่อาจไม่สามารถป้องกันอาชญากรรายใหม่

5. การใช้แฟ้มข้อมูลประวัติไม่ดีร่วมกัน

ร้านค้าหลายรายสามารถที่จะใช้แฟ้มข้อมูลประวัติไม่ดีร่วมกัน เนื่องจากฐานข้อมูลนี้จะได้ข้อมูลมาจากร้านค้าหลายๆ ราย ฉะนั้นการใช้ฐานข้อมูลนี้จะช่วยลดการก่ออาชญากรรม โดยเฉพาะอาชญากรรมที่มีลักษณะเฉพาะตัว ข้อเสียของวิธีนี้ก็คือลูกค้าที่ไม่ดีของร้านค้ารายหนึ่งอาจจะไม่ใช่ลูกค้าที่ไม่ดีของร้านค้ารายอื่นๆ

6. เงื่อนไขที่สามารถปรับเปลี่ยนได้ของผู้ค้า

ร้านค้าตั้งเงื่อนไขขึ้นเพื่อหยุดหรือส่งสัญญาณให้ตรวจสอบคำสั่งซื้อใดคำสั่งซื้อหนึ่ง ตัวอย่างเช่น ร้านค้าอาจจะตั้งเงื่อนไขให้ตรวจสอบคำสั่งซื้อที่มาจาก IP address หรือประเทศใดประเทศหนึ่ง หรือคำสั่งซื้อที่มีมูลค่ามากกว่าจำนวนใดจำนวนหนึ่ง หรือให้ส่งไปยังที่อยู่ใดที่อยู่หนึ่งโดยเฉพาะเจาะจง วิธีนี้อาจจะส่งสัญญาณให้มีการตรวจสอบลูกค้าที่ปกติด้วย แต่จะช่วยลดการทำผิดซ้ำ หรือการกระทำผิดรูปแบบใดรูปแบบหนึ่งโดยเฉพาะ หากเป็นกรณีที่ IP adress เปลี่ยนไปเรื่อยๆ ตามแต่ ISP จะจัดสรรให้ อาจส่งผลให้คำสั่งซื้อที่ปกติเกิดความล่าช้าหรือถูกปฏิเสธ

7. ระบบการให้คะแนนอาชญากรรม

วิธีนี้ร้านค้าจะให้คะแนนองค์ประกอบต่างๆ ในธุรกรรม (IP address, บริการ Free E-mail, เวลาที่สั่งซื้อ, ผลของ AVS, จำนวนสินค้า, วิธีการส่งสินค้า, ความแตกต่างของที่อยู่บนบัตรกับที่อยู่ที่ให้จัดส่งสินค้า ฯลฯ) เพื่อให้คะแนนอาชญากรรม เพื่อบ่งชี้ความเป็นไปได้ของอาชญากรรม อันส่งผลให้ร้านค้าสามารถตัดสินใจได้ว่าจะปฏิเสธคำสั่งซื้อไหน ตรวจสอบว่า IP address ตรงกับที่อยู่บนบัตรของลูกค้าหรือไม่ อาชญากรรมจำนวนมากจะมาจากบริการอีเมล์ฟรี บริษัทหลายๆ บริษัทปฏิเสธคำสั่งซื้อที่มาจากบริการอีเมล์ฟรี หรืออีเมล์ที่เป็นเว็บเบส หรือโดเมนที่ไม่ได้เป็น ISP โดยความเป็นจริงแล้วทุกๆ คนที่ใช้บริการอีเมล์ฟรี หรืออีเมล์ที่เป็นเว็บเบส หรือที่อยู่

แบบ forward จะต้องมี ISP ที่สามารถสืบทราบได้ คำสั่งซื้อที่เป็นอาชญากรรมในสหรัฐจะเกิดขึ้นในช่วง เที่ยงคืนถึงตีสองโดยให้ระวังคำสั่งซื้อที่ให้มีการจัดส่งในทันทีหรือวันต่อไป อาชญากรจะไม่สนใจกับค่าใช้จ่ายที่เพิ่มขึ้น เพราะว่าพวกเขาไม่ได้จ่ายเงินอยู่แล้ว ความเสี่ยงที่จะเป็นอาชญากรรมจะมากขึ้นถ้าที่อยู่บนบัตรไม่ตรงกับที่อยู่ที่ให้จัดส่งสินค้า ร้านค้าบางรายเริ่มใช้บริการการตรวจสอบอาชญากรรม และซอฟต์แวร์นิรภัยเพื่อประเมินความเสี่ยง ร้านค้าสามารถที่จะตัดสินใจว่าจะรับหรือปฏิเสธบัตรเครดิตจากค่าที่ประเมินได้ ร้านค้ารายใหญ่บางรายสร้างระบบการให้คะแนนของตนเองโดยใช้ข้อมูลประวัติอาชญากรรมและการไม่ชำระเงิน วิธีการโดยเฉพาะนี้น่าจะกำจัดอาชญากรรมได้มากขึ้น แต่ต้องใช้เวลา และเงินมากขึ้นในการติดตั้งซอฟต์แวร์ใหม่

8. ระบบการติดตามลูกค้า

ร้านค้าจะติดต่อลูกค้าโดยการโทรศัพท์หรืออีเมล์เพื่อขอข้อมูลเพิ่มเติมถ้าคำสั่งซื้อนั้นน่าสงสัย ร้านค้าจะถามชื่อของธนาคารบนบัตร หรือที่อยู่บนบัตรอย่างครบถ้วน ซึ่งวิธีนี้จะต้องใช้เวลาและเงินมากขึ้น แต่อาชญากรจะไม่สามารถตอบคำถามได้ถูกต้อง แต่ผู้ที่เคยเห็นบัตรจะสามารถบอกข้อมูลได้ทันที ถ้าโทรไปถามผู้ออกบัตร เขาก็จะสามารถแจ้งชื่อและหมายเลขโทรศัพท์ของธนาคารที่ออกบัตรได้ ปัจจุบันมีบริการรายชื่อหลายรายบนอินเตอร์เนทที่สามารถเข้าไปหาชื่อและที่อยู่ได้ฟรี หรือจะจัดซื้อ CD รายนามโทรศัพท์ที่มีคุณภาพ เพื่อใช้ในการตรวจสอบหมายเลขโทรศัพท์และที่อยู่ หรือพิจารณาที่จะซื้อเครื่องบอกเบอร์ผู้โทรเข้า (Caller ID) เพื่อตรวจสอบชื่อและหมายเลขโทรศัพท์ ถ้าที่อยู่บนบัตรต่างจากที่อยู่ในการจัดส่งสินค้า ควรขอเบอร์โทรศัพท์ของทั้งสองที่

9. กระบวนการหลังรับคำสั่งซื้อ

ร้านค้าจะได้รับอีเมล์ยืนยันการซื้อสินค้าภายใน 30 นาที ซึ่งในเวลา 30 นาทีนั้น ร้านค้าสามารถที่จะตรวจสอบหมายเลขบัตรเครดิตเพื่อหาความเป็นไปได้ของอาชญากรรม วิธีนี้ไม่ก่อให้เกิดขั้นตอนมากขึ้นทั้งกับลูกค้า และร้านค้า ซึ่งอาจจะนำไปสู่การสูญเสียยอดขาย หากร้านค้าได้รับคำสั่งซื้อจากอีเมล์ที่ให้บริการฟรี ให้ส่งอีเมล์กลับไปเพื่อขอข้อมูลเพิ่มเติมก่อนที่จะดำเนินการ ให้ลูกค้าส่งที่อยู่อีเมล์ที่ไม่ได้เป็นบริการฟรี ชื่อ และหมายเลขโทรศัพท์ของธนาคารที่ออกบัตร ชื่อนามสกุลที่อยู่บนบัตรของผู้ถือบัตรและที่อยู่ที่สมบูรณ์ตามบัตร ถ้าได้รับข้อมูลเพิ่มเติมแล้วร้านค้าสามารถตรวจสอบข้อมูลเหล่านั้นได้ หรือร้านค้าอาจจะใช้นโยบาย "การยืดเวลาการจัดส่งสินค้า" สำหรับคำสั่งซื้อสินค้าปริมาณมากๆ ทั้งนี้อาชญากรรมบัตรเครดิตจะถูกรายงานภายใน 24 ชั่ว

โมง หรืออาจใช้เวลาถึง 24 ชั่วโมงในการที่จะบันทึกหมายเลขบัตรที่ถูกรายงานว่าเป็นการกระทำอาชญากรรมลงในฐานข้อมูล นอกจากนี้ควรจะให้มีการลงลายมือชื่อรับสินค้า เมื่อสินค้าถูกส่งออกไป (FEDEX, UPS และกรมไปรษณีย์) ถ้าร้านค้าขอชื่อและหมายเลขโทรศัพท์ของธนาคารที่อยู่บนบัตร ก็จะสามารถตรวจสอบได้ว่าผู้ที่ส่งคำสั่งซื้อนั้นเป็นผู้มีสิทธิใช้บัตรนั้นหรือไม่

หน้าแสดงความขอบคุณที่ไม่ใช้ภาษาอังกฤษ ถ้าสินค้านั้นถูกส่งไปยังประเทศที่ไม่ใช้ภาษาอังกฤษเป็นภาษาหลัก บนเว็บไซต์ควรจะมีหน้าแสดงความขอบคุณที่ไม่ใช้ภาษาอังกฤษ อธิบายให้ลูกค้าจัดส่งโทรสารสำเนาบัตรเครดิตหรือสำเนาใบแจ้งหนี้ของบัตรเครดิตที่ใช้ หากลูกค้าไม่ดำเนินการดังกล่าวจะต้องถูกหักเงินจำนวนหนึ่งจากยอดรวมที่สั่งซื้อ

ซอฟต์แวร์ที่ได้รับการออกแบบมาโดยเฉพาะ ร้านค้าบางรายให้ซอฟต์แวร์แสดงชื่อของลูกค้าลงในซอฟต์แวร์ด้วย ซึ่งจะต้องมีการรวบรวมรหัสก่อนที่จะใช้กับลูกค้า เมื่อรายงานพิมพ์ออกมาก็จะมีชื่อลูกค้าที่ได้รับอนุญาต หรือสถาบันที่ซื้อใบอนุญาตของเว็บไซต์นั้น อาจจะมีการให้รหัสผ่านที่สามารถใช้ได้ชั่วคราว 30 วัน แก่ซอฟต์แวร์ที่ได้รับการดาวน์โหลด รหัสผ่านถาวรจะถูกอีเมล์ไปยังลูกค้าภายใน 2-3 สัปดาห์ถัดไป เมื่อมีการตรวจสอบทุกอย่างเกี่ยวกับอาชญากรรมแล้ว การส่งรหัสผ่านถาวรอาจจะใช้ระบบอัตโนมัติเพื่อช่วยประหยัดเวลา

10. **การอนุมัติแบบ** Real-time

ข้อมูลบัตรเครดิตจะถูกส่งไปยังผู้ดำเนินการเพื่อการอนุมัติในทันที (ปกติ 5 วินาทีหรือน้อยกว่า) วิธีนี้ตรวจสอบว่าบัตรเครดิตนั้นไม่ได้ถูกแจ้งอายัดไว้ และหมายเลขนั้นถูกต้อง ลูกค้ายังอยู่ในขั้นตอนการติดต่อกับร้านค้า และข้อมูลที่ผิดพลาดก็จะได้รับการแก้ไขให้ถูกต้อง ซึ่งการอนุมัติแบบ Real-time นี้ จะมีค่าใช้จ่ายเพิ่มขึ้น การอนุมัตินี้ไม่ได้บอกว่าผู้ที่ใช้บัตรเครดิตนั้นเป็นผู้ที่มีสิทธิใช้หรือไม่

11. ฐานข้อมูลการบริการเกี่ยวกับเครดิต

บริการฐานข้อมูลเครดิต เช่น Equifax, Experian และ Trans Union นั้นเหมาะสมที่สุดกับสินค้าที่มีราคาสูง ลูกค้าจะต้องแจ้งข้อมูลที่เฉพาะเจาะจงมากๆ เช่น นามสกุลของมารดา หรือหมายเลขประกันสังคม แต่บริการดังกล่าวอาจจะมีราคาแพงและใช้เวลานาน องค์กรบางองค์กร เช่น www.antifraud.com ให้บริการที่ถูกกว่า (10 เหรียญต่อเดือน)

12. แฟ้มข้อมูลประวัติดี

เป็นแฟ้มข้อมูลของลูกค้าที่มีคุณสมบัติที่ดี เช่น ลูกค้าที่สามารถอัพเกรดการซื้อ ลูกค้าที่มีการซื้อขายที่สมบูรณ์ถูกต้องในอดีตนั้นจะมีแนวโน้มที่จะไม่เป็นอาชญากรรม ซึ่งควรจะมีจำกัดบุคคลที่สามารถเข้าถึงข้อมูลในแฟ้มข้อมูลนี้ ซึ่งควรจะมีการใช้รหัสผ่าน

13. การตรวจจับรูปแบบ

ตรวจสอบว่ามีคำสั่งซื้อหลายๆ คำสั่งให้ส่งไปยังที่อยู่เดียวกัน จากบัตรเครดิตหลายๆ ใบหรือไม่ เพราะอาชญากรอาจจะมีข้อมูลหมายเลขบัตรเครดิตที่ขโมยมาหลายใบ ถ้าหมายเลขบัตรเครดิตต่างกันเพียงไม่กี่ตัวเลข หมายความว่ามีความเป็นไปได้สูงว่าหมายเลขนั้นได้มาจากโปรแกรมคอมพิวเตอร์ ตรวจสอบว่ามีการส่งคำสั่งซื้อหลายคำสั่งมาจาก IP address เดียวกันหรือไม่ หรือเป็นกรณีที่ผู้ใช้บัตรใช้หมายเลขบัตรเครดิตเดียวกันแต่แจ้งวันหมดอายุของบัตรต่างกันไป ในหลายๆ กรณีอาชญากรอาจจะมีหมายเลขบัตรเครดิต แต่ไม่มีวันหมดอายุ ฉะนั้นคนเหล่านั้นก็จะพยายามใช้หมายเลขบัตรกับวันหมดอายุที่ต่างๆ กันจนกว่าจะได้วันที่ถูกต้อง นอกจากนี้ยังควรตรวจสอบคำสั่งซื้อของสินค้าประเภทเดียวที่มีคำสั่งในปริมาณมากๆ

14. มาตรการการป้องกัน

ตรวจสอบข้อมูลในช่องกรอกข้อมูลว่าผู้ซื้อเป็นตัวจริงหรือไม่ โดยอาจตรวจสอบว่ารหัสไปรษณีย์ที่ลูกค้าใส่นั้นมีจริงหรือไม่ ตรวจสอบที่อยู่อีเมล์ที่ลูกค้าให้ว่ามีฟอร์มที่ถูกต้อง ตรวจสอบข้อมูลที่น่าสงสัย เช่น ชื่อลูกค้า นายสมชาย สายชม หรือนางสาวมานี มีนา หรือที่อยู่ เช่น บ้านเลขที่12345 ถนนใหญ่ นอกจากนี้ควรให้ความรู้แก่พนักงานโดยการให้เข้าร่วมสัมมนาที่จัดโดยบริษัทบัตรเครดิต หรือผู้ดำเนินการบัตรเครดิต ลงข้อความในเว็บไซต์ว่ามีระบบป้องกันการก่ออาชญากรรม และจะดำเนินคดีอย่างถึงที่สุดกับอาชญากร และแจ้งว่าคุณจะแจ้งการกระทำผิดทุกรายการต่อสำนักงานตำรวจแห่งชาติ.