บทที่ 3
ระบบการเงินของพาณิชย์อิเล็กทรอนิกส์

3.1 ระบบชำระเงินของพาณิชย์อิเล็กทรอนิกส์

ระบบการชำระเงินผ่านอินเทอร์เน็ต ได้รับการพัฒนาขึ้นมาหลายระบบ โดยแต่ละระบบจะมีกระบวนการและคุณสมบัติด้านความปลอดภัยและความสะดวกแตกต่างกันไป ระบบที่ใช้แพร่หลายในปัจจุบัน คือ การใช้บัตรเครดิต เนื่องจากการจ่ายเงินกันตามร้านค้าธรรมดา ทั้งทางผู้ซื้อและผู้ขายก็ใช้บัตรเครดิตกันแพร่หลายอยู่แล้ว การนำระบบนี้ไปใช้บนอินเทอร์เน็ต จึงไม่ยุ่งยากนัก เพราะผู้ใช้เข้าใจระบบดีอยู่แล้ว

นอกจากบัตรเครดิตแล้ว ก็ยังมีระบบจ่ายเงินอื่น ๆ อีก ซึ่งอาจจะมีความสำคัญมากขึ้น ในอนาคตเช่นกัน ระบบเหล่านี้มีจุดเด่นจุดด้อยต่างกัน ดังนี้

3.1.1 บัตรเครดิต (Credit Cards)

ระบบบัตรเครดิตทำงานในลักษณะที่ผู้ซื้อไม่ต้องจ่ายเงินของตัวเองทันทีเมื่อซื้อสินค้า โดยผู้ซื้อจะได้รับเครดิต จากธนาคารผู้ออกบัตรให้ไปก่อน แล้วจึงชำระบัญชีกับธนาคารของตนทุกเดือน ส่วนผู้ขายจะได้รับชำระเงินทันทีภายในหนึ่งวันหลังการซื้อขาย โดยผ่านธนาคารของผู้ขายเอง

กระบวนการทำงานของบัตรเครดิตธรรมดาเป็นดังนี้ เมื่อผู้ถือบัตรให้บัตรเครดิต หรือหมายเลขบัตรแก่ผู้ขาย ผู้ขายก็จะร้องขอให้ธนาคารของผู้ขายอนุมัติเครดิตของผู้ซื้อทางธนาคารผู้ขายก็จะส่งคำร้องขอต่อไปยังเครือข่ายบัตรเครดิต (เช่น เครือข่ายของวีซ่าหรือมาสเตอร์การ์ด) ซึ่งจะส่งคำร้องขอต่อไปถึงธนาคารของผู้ซื้อ ธนาคารผู้ซื้อจะตรวจสอบเครดิตของผู้ซื้อแล้วส่งคำตอบผ่านเครือข่ายกลับไปว่าอนุมัติเครดิตหรือไม่ โดยคำตอบนี้จะส่งไปถึงผู้ขายในที่สุด

การใช้บัตรผ่านอินเทอร์เน็ต จะแตกต่างจากธรรมดาตรงที่ ทั้งผู้ซื้อผู้ขายไม่รู้ตัวตนของกันและกันอย่างแน่ชัด ดังนั้นจึงมีความพยายามจะสร้างความปลอดภัยในการส่งหมายเลขบัตรเครดิตไปยังผู้ขายและเป็นผลให้เกิดวิธีการที่แตกต่างกันไป

การชำระเงินด้วยบัตรเครดิต จะใช้ protocol อยู่ 2 แบบ คือ Secure Sockets Layer (SSL) และ Secure Electronic Transactions (SET) ซึ่งแต่ละวิธีก็มีข้อดีและข้อเสียแตกต่างกัน คือ SSL ให้บริการในการ Encrypt และ Decrypt ข้อมูลระหว่าง Web Browser และ Web Server โดยใช้ Protocol HTTPS และ Server Authentication ซึ่งผู้ใช้งานไม่จำเป็นต้องมี Certificate และมีค่าใช้จ่ายในการพัฒนาที่ถูกกว่า

ระบบ SET ส่วนระบบ SET เองนั้น ทั้งผู้ใช้หรือลูกค้า , ร้านค้า และ ธนาคารที่ร้านค้าติดต่อด้วย จะต้องมี Certificate ทั้งหมด และในส่วนของการ Encrypt และ Decrypt นั้น จะทำเป็น 2 ส่วน คือ ระหว่างลูกค้ากับร้านค้า เป็นส่วนที่หนึ่ง และ ระหว่างลูกค้าและธนาคาร เป็นส่วนที่สอง คือ ร้านค้าจะไม่เห็นข้อมูลเกี่ยวกับการชำระเงินของลูกค้า แต่จะเห็นเพียงรายการสั่งซื้อสินค้าเท่านั้น ส่วนธนาคารจะเห็นข้อมูลการชำระเงิน เช่น หมายเลขบัตรเครดิต เป็นต้น แต่จะไม่เห็นข้อมูลการสั่งซื้อสินค้า ซึ่งระบบ SET นั้น จะกระทำผ่านทาง Virtual Private Networks (VPN) ซึ่งทำให้ระบบนี้ มีต้นทุนในการพัฒนาและใช้งานสูง แต่มีความน่าเชื่อถือ และปลอดภัยมากกว่า ระบบ ที่ใช้ SSL

วิธีการจ่ายเงินผ่านบัตรเครดิต บนอินเทอร์เน็ต มีหลายวิธีดังนี้

1. ส่งหมายเลขบัตรเครดิตที่ไม่ได้เข้ารหัสไปยังเว็บไซต์ของผู้ขายโดยผู้ซื้อจะใส่หมายเลขบัตรเครดิตเข้าไปในแบบฟอร์มบนเว็บไซต์ของผู้ขายแล้วส่งข้อมูลไปวิธีนี้เป็นวิธีที่ปลอดภัยน้อยที่สุด เนื่องจากหมายเลขบัตรที่ส่งไปอาจถูกดักเอาไปได้ระหว่างทาง
2. ส่งหมายเลขบัตรเครดิต ที่เข้ารหัสแล้วไปยังเว็บไซต์ของผู้ขาย แตกต่างจากวิธีแรกตรงที่มีการเข้ารหัสหมายเลขบัตรเครดิตก่อนส่งไปด้วยเมื่อข้อมูลไปถึงเว็ปไซต์ของผู้ขายก็จะถูกถอดรหัสออกไปเพื่ออ่านหมายเลขบัตรโดยทั่วไปจะใช้ SSL Protocol เพื่อทำการเข้ารหัสและถอดรหัส

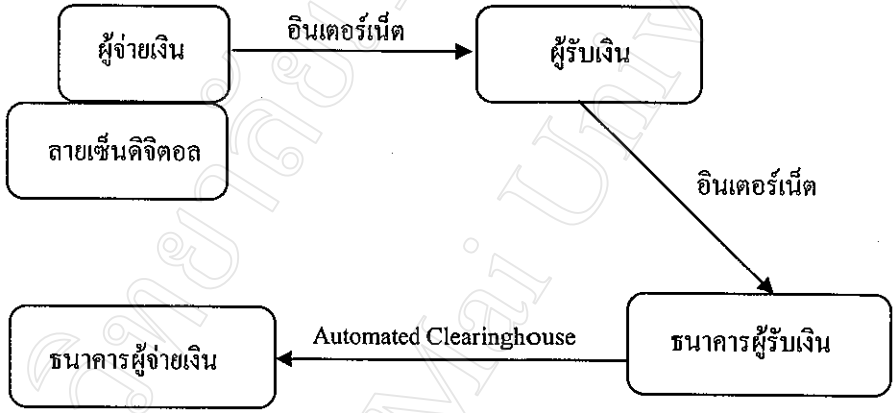
วิธีนี้ปลอดภัยกว่าวิธีแรกเนื่องจากผู้ที่ดักข้อมูลไประหว่างทางจะไม่สามารถอ่านหมายเลขบัตรได้แต่ผู้ใช้ยังมีความเสี่ยงในแง่ที่ผู้ขายทุกรายที่ติดต่อด้วยจะทราบหมายเลขบัตรเครดิตของตนและอาจนำไปใช้ผิด ๆ ได้ หรือหากเว็บไซต์ของผู้ขายมีระบบรักษาความปลอดภัยไม่ดี อาจมีผู้เจาะระบบเข้าไปเอาหมายเลขบัตรออกมาได้ (การเข้ารหัสด้วย SSL Protocol จะช่วยรักษาความปลอดภัยของข้อมูลระหว่างทางเท่านั้น เมื่อไปถึงปลายทางแล้ว ก็จะขึ้นอยู่กับระบบรักษาความปลอดภัยที่นั่น)

3.1.2 เช็คอิเล็กทรอนิกส์ (Electronic Checks)

เช็คอิเล็กทรอนิกส์เป็นระบบที่ทำงานคล้ายกับการใช้เช็คธรรมดา แต่เปลี่ยนสื่อที่ใช้กระดาษมาเป็นสื่ออิเล็กทรอนิกส์แทน กระบวนการใช้งานก็เหมือนการใช้เช็คธรรมดานั่นคือ ผู้จ่ายเงินจะเขียนเช็คแล้วเซ็นรับรอง ว่าเป็นเช็คของตน ต่อจากนั้นก็จะส่งเช็คนี้ไปให้ผู้รับเงิน แล้วผู้รับเงินก็จะนำเช็คนี้ไปแสดงต่อธนาคารของตนเพื่อนำเงินเข้าบัญชี และธนาคารของผู้รับเงินก็จะไปชำระบัญชีกับธนาคารของผู้จ่ายเงิน โดยผ่านทางเครือข่ายการชำระบัญชีที่เรียกว่า Automated Clearing house ซึ่งหากว่าผู้เซ็นเช็คมีเงินอยู่ในบัญชีจริงเงินก็จะถูกโอนส่งผ่านมาเข้าบัญชีของผู้รับเงินในที่สุด

ในระบบเช็คอิเล็กทรอนิกส์ที่พัฒนาขึ้นโดย FSTC (Financial Services Technology Consortium Inc.) ผู้จ่ายเงินจะใช้เครื่องมือที่เป็นฮาร์ดแวร์ เช่น Smart Card เพื่อเซ็นเช็คโดยใช้ลายเซ็นดิจิตอล ของตน ลายเซ็นดิจิตอลนี้เป็นรหัสพิเศษที่สร้างขึ้นโดยใช้วิธีการเข้ารหัสที่ทำให้ผู้อื่นไม่สามารถปลอมแปลงได้ จากนั้น ก็จะส่งเช็คอิเล็กทรอนิกส์ ไปยังผู้รับเงินโดยผ่านทางเครือข่ายคอมพิวเตอร์ ผู้รับเงินก็จะเซ็นรับรองโดยใช้ลายเซ็นดิจิตอลของตน แล้วนำเช็คอิเล็กทรอนิกส์นี้ไปเข้าธนาคารซึ่งธนาคารผู้รับเงินก็จะไปชำระบัญชีผ่านทางเครือข่าย Automated Clearing house ตามระบบเดิม

รูปที่ 3.1 แผนภูมิกระบวนการทำงานของการใช้เช็คอิเล็กทรอนิกส์



ระบบเช็คอิเล็กทรอนิกส์นี้ ออกแบบมาให้ใช้ฮาร์ดแวร์ในการเขียนลายเซ็นดิจิตอลเพื่อกำกับเช็ค ทั้งนี้เพื่อให้มีความปลอดภัยสูง ถ้าหากใช้ซอฟต์แวร์แต่เพียงอย่างเดียวในการเขียนลายเซ็นดิจิตอลอาจถูกเจาะระบบเพื่อขโมยลายเซ็นได้ง่ายกว่า

จุดที่เช็คอิเล็กทรอนิกส์น่าจะอำนวยความสะดวก และเพิ่มประสิทธิภาพในการทำงานได้มากที่สุดก็คือการส่งเช็กผ่านทางระบบเครือข่ายอินเทอร์เน็ตแทนที่จะใช้จดหมายเพื่อส่งเช็คระหว่างผู้จ่ายเงินและผู้รับเงิน หรือการเอาเช็คเดินไปเข้าธนาคาร แต่ระบบเช็คอิเล็กทรอนิกส์ยังไม่แพร่หลายในปัจจุบัน

3.1.3 เงินสดอิเล็กทรอนิกส์หรือเงินสดดิจิตอล (Electronic Cash or Digital Cash)

เงินสดมีคุณสมบัติที่เหนือกว่าการจ่ายเงินแบบวิธีอื่นๆ อยู่หลายอย่าง ทั้งในด้านความรวดเร็ว เนื่องจากไม่ต้องรอการชำระบัญชี ความเป็นมาตรฐานเพราะทุกฝ่ายยินดีรับเงินสดและความเป็นส่วนตัว เพราะการใช้เงินสดไม่มีการบันทึกข้อมูลเอาไว้เหมือนบัตรเครดิตหรือเช็ค ดังนั้นจึงมีหลายฝ่ายที่พยายามสร้างระบบเงินสดดิจิตอลขึ้นมา เพื่อรวมเอาคุณสมบัติของเงินสดเข้ากับความสะดวกในการส่งเงินสดดิจิตอลผ่านทางระบบเครือข่ายคอมพิวเตอร์โดยเฉพาะอินเทอร์เน็ต

เงินสดดิจิตอลเป็นเพียงตัวเลขหรือรหัสที่สร้างขึ้นจากคอมพิวเตอร์ที่ใช้แทนเงินสดได้ แน่นอนว่าจะต้องมีผู้รับรองค่าของเงินสดดิจิตอลเหล่านี้ บริษัทที่สร้างเทคโนโลยีเงินสดดิจิตอล เช่น DigiCash หรือ CyberCash จึงร่วมมือกับธนาคารและผู้ขายสินค้ารายต่างๆเพื่อให้ยอมรับการใช้เงินสดลักษณะนี้

ผู้ที่พิมพ์เงินสดดิจิตอลเหล่านี้ โดยทั่วไปแล้วคือ ธนาคาร โดยธนาคารจะกำหนดหมายเลขของเงินสดดิจิตอลเหล่านี้แล้วเซ็นกำกับด้วยลายเซ็นดิจิตอลของธนาคาร เมื่อผู้ใช้ได้รับเงินสดดิจิตอลแล้ว ก็สามารถที่จะนำไปใช้ได้กับพ่อค้าหรือบุคคลอื่นๆที่ยอมรับเงินสดดิจิตอลนั้น โดยผู้รับเงินก็สามารถตรวจสอบความถูกต้องของเงินสดดิจิตอลได้โดยใช้วิธีการถอดรหัสรายเซ็นดิจิตอลออกมาดู (ในระบบการเข้ารหัสแบบนี้ รหัสที่ใช้ในการเซ็นกำกับเงินสดดิจิตอล กับรหัสที่ใช้ในการถอดรหัสเพื่อตรวจสอบความถูกต้องของเงินนั้น เป็นคนละตัวกัน จึงไม่ต้องห่วงว่าจะมีผู้อื่นปลอมเป็นธนาคารแล้วสร้างเงินสดดิจิตอลปลอมออกมาได้)

จุดเด่นอีกข้อหนึ่งของเงินสดดิจิตอลก็คือ " การมีค่าใช้จ่ายในการประมวลผลต่ำ " การใช้บัตรเครดิตจะมีต้นทุนการประมวลผลสูงถึง 40 เซ็นต่อหนึ่งรายการ ดังนั้นถ้าผู้ใช้ต้องการซื้อของที่มีมูลค่าต่ำๆก็ไม่คุ้มที่จะจ่ายเงินด้วยบัตรเครดิตได้ แต่เงินสดดิจิตอลมีต้นทุนในการประมวลผลต่ำกว่ามาก จึงทำให้การจ่ายเงินให้กับสิ่งเล็กๆน้อยเช่น ค่าอ่านบทความหนึ่งเรื่องสามารถทำได้ เราเรียกการจ่ายเงินลักษณะนี้ว่า Micropayment

ปัจจุบันการใช้เงินสดดิจิตอลก็ยังไม่เป็นที่แพร่หลายเช่นกันปัญหาสำคัญก็คือการไม่มีมาตรฐานที่เข้ากันได้ระหว่างเทคโนโลยีเงินสดดิจิตอลต่างๆ ซึ่งผู้ใช้เงินสดดิจิตอลยี่ห้อหนึ่งๆยังไม่สามารถที่จะแลกเปลี่ยนกับเงินสดยี่ห้ออื่นได้อย่างอิสระ นอกจากนี้ก็ยังมีปัญหาที่ผู้บริโภคจะต้องใช้ในการทำความเข้าใจ และให้ความไว้วางใจกับเทคโนโลยีใหม่อย่างเงินสดดิจิตอลอีกด้วย

ในอนาคตปัญหาเรื่องมาตรฐานอาจได้รับการแก้ไขในที่สุด โดยบริษัทเทคโนโลยีเงินสดดิจิตอล 30 แห่งได้เริ่มทำความตกลงกันที่จะวางมาตรฐานร่วมกันเพื่อให้เงินสดดิจิตอลรูปแบบต่างๆ ใช้งานร่วมกันได้

3.1.4 Smart Card

การชำระเงินด้วย Smart Card เป็นวิธีที่ ลูกค้านำเงินสดไปฝากเข้าในบัญชีบัตร Smart Card ที่มีอยู่กับธนาคารก่อน จากนั้น ก็ Update ข้อมูลยอดเงินบนบัตร ก่อนนำไปใช้ เมื่อจะใช้งาน ลูกค้าจะต้องใส่บัตรนี้ ลงในเครื่องอ่านบัตร ขณะจะชำระเงิน เพื่อส่งข้อมูลบนบัตรให้กับร้านค้าที่ซื้อสินค้า จากนั้นร้านค้าจะนำข้อมูลนี้ ไปตรวจสอบและเรียกเก็บกับธนาคารเจ้าของบัตร จากนั้น ร้านค้าจึงจะส่งสินค้าให้กับลูกค้า

Smart Card เป็นบัตรขนาดเล็กที่มีชิปคอมพิวเตอร์ติดอยู่ ตรงนี้เป็นจุดที่แตกต่างจากบัตรแม่เหล็กธรรมดา ซึ่งชิปนี้ใช้เพื่อเก็บข้อมูลของผู้ใช้ หรือใช้เก็บจำนวนเงินและ Smart Card บางประเภทก็สามารถประมวลผลข้อมูลได้ด้วย โดยส่วนใหญ่ความสามารถในการประมวลผลนี้จะใช้เพื่อเข้ารหัสและถอดรหัสของข้อมูลผู้ใช้ ซึ่งทำให้ Smart Card มีความเป็นส่วนตัวและปลอดภัยมากเป็นพิเศษ

การประยุกต์ใช้ Smart Card ที่สำคัญมีหลายอย่าง เช่น ในระบบโทรศัพท์ของประเทศต่างๆทั่วโลก ได้หันมาใช้ Smart Card ที่มีจำนวนเงินเก็บไว้ก่อน แล้วแทนการใช้เหรียญ ตัวอย่างในประเทศไทย เช่น TOT Card นอกจากนี้ยังมีการใช้ Smart Card แทนเงินสดในที่จอดรถ ระบบขนส่งมวลชน เป็นต้น

ในระบบสาธารณะสุข Smart Card ได้ถูกนำไปใช้เพื่อเก็บข้อมูลทางการแพทย์ ซึ่งทำให้ขนไข้สามารถเก็บข้อมูลประวัติทางการแพทย์ของตนเองไว้ใกล้ตัว และสะดวกที่จะนำไปใช้ได้ในสถานรักษาพยาบาลต่างๆ หรือทำให้หน่วยฉุกเฉินทราบข้อมูลได้ทันท่วงทีในกรณีเกิดอุบัติเหตุ และ Smart Card ก็ยังเป็นเครื่องมือในการควบคุมทางด้านความปลอดภัย และการจ่ายเงินของโทรศัพท์มือถือระบบ GSM ด้วย

Smart Card มีศักยภาพที่จะใช้ในการจ่ายเงินผ่านอินเทอร์เน็ตได้ โดยมีจุดเด่นที่ทำให้เกิดความปลอดภัยมากกว่า และสามารถพกพาไปที่ต่างๆได้ง่าย และเป็นส่วนตัว หากสถานที่นั้นมีเครื่องอ่านบัตร Smart Card แล้วผู้ใช้ก็สามารถดึงข้อมูลของตน หรือจำนวนเงินที่เก็บเอาไว้ในบัตรมาใช้ได้โดยง่าย

ปัจจุบัน Smart Card ได้ถูกนำไปใช้อย่างกว้างขวางที่สุดทางประเทศทางยุโรป และกำลังแพร่หลายมากขึ้นไปในประเทศอื่นๆทั่วโลก

3.1.5 การจ่ายเงินโดยผ่านบริการของบุคคลที่สามที่เชื่อถือ (Trusted Third Party)

วิธีการนี้ช่วยแก้ไขจุดอ่อนของระบบที่สอง โดยวิธีนี้ผู้ขายไม่ทราบบัตรเครดิตของผู้ซื้อทำให้ลดความกังวลเรื่องการติดต่อกับผู้ขายที่ไม่ได้รู้จักกับตนมาก่อน หมายเลขบัตรเครดิตาของผู้ซื้อจะถูกส่งไปหรือถูกเก็บไว้ที่องค์กรที่ทำหน้าที่ประมวลผลบัตรเครดิตโดยเฉพาะ เช่น Cyber Cash หรือ First Virtual ด้วยวิธีที่ปลอดภัย เมื่อผู้ซื้อต้องการซื้อสินค้าก็จะไม่ต้องส่งหมายเลขบัตรเครดิตไปให้กับร้านค้าโดยตรง แต่ร้านค้าจะสอบถามความถูกต้องของบัตรเครดิตของผู้ซื้อผ่านองค์กรเหล่านี้ แล้วองค์กรเหล่านี้จะทำหน้าที่ขออนุมัติการใช้บัตรเครดิตกับธนาคารของผู้ซื้อ หากได้รับอนุมัติก็จะบอกกลับไปยังผู้ขายแล้วผู้ขายก็จะขายสินค้าให้กับผู้ซื้อคนนี้ได้

วิธีการนี้ให้ความปลอดภัยสูงกว่าการซื้อขายในร้านค้าทั่วไปเสียอีกเนื่องจากหมายเลขบัตรเครดิตจะไม่ผ่านมือใครเลย นอกจากองค์กรประมวลผลบัตรเครดิตที่เราติดต่อด้วยองค์กรเหล่านี้ทำหน้าที่ด้านนี้โดยเฉพาะจึงมีระบบรักษาความปลอดภัยที่สูงมาก

อย่างไรก็ดีวิธีนี้ยังไม่แพร่หลายนักเนื่องจากยังไม่มีมาตราฐานที่เป็นหนึ่ง องค์กรเหล่านี้มีหลายแห่งและยังคงแข่งขันกันอยู่

ระบบการจ่ายเงินโดยผ่านบริการของบุคคลที่สามที่เชื่อถือที่น่าสนใจและกำลังมาแรงอันหนึ่งเป็นของ paypal.com ซึ่งทำให้การจ่ายเงินระหว่างบุคคลกับบุคคลสามารถทำได้โดยสะดวก ระบบ Paypal ทำให้ผู้ใช้สามารถส่งเงินสดไปให้ใครก็ตามในประเทศสหรัฐอเมริกาได้โดยเพียงแต่ใช้อีเมล์เท่านั้นซึ่งผู้ใช้ระบบก็เพียงแต่ลงทะเบียนกับ Paypal ไว้ แล้วจากนั้นเมื่อต้องการจะจ่ายเงินให้กับใครผู้จ่ายเงินก็ใส่หมายเลขบัตรเครดิตของตนและจำนวนเงินที่ต้องการจ่ายเข้าไป บัตรเครดิตของผู้จ่ายก็จะถูกชาร์จ แล้ว Paypal จะสร้างบัญชีของผู้รับเงินเอาไว้ให้มีเงินตามจำนวนที่ได้รับ และส่งอีเมล์ไปให้ผู้รับเงินทราบ ผู้รับเงินสามารถเลือกที่จะถอนเงินออกไปได้ โดยให้ Paypal ฝากเงินเข้าบัญชีธนาคารของตนส่งเช็คไปให้ หรืออาจจะเก็บเงินนี้ไว้ที่ Paypal แล้วนำไปใช้ส่งให้ผู้ใช้คนอื่นต่อก็ได้

นอกจากจ่ายเงินโดยใช้บัตรเครดิตแล้ว ผู้จ่ายเงินอาจเลือกที่จะนำเงินเข้าบัญชี Paypal ของตนโดยวิธีอื่นก็ได้ด้วยการใช้เช็คหรือการหักเงินจากบัญชีธนาคาร

บริการนี้เป็นบริการฟรี ทั้งผู้จ่าย และผู้รับเงินไม่ต้องจ่ายค่าธรรมเนียมอะไรเลย รายได้ของ Paypal จะมาจากดอกเบี้ยของเงินที่ค้างอยู่ในบัญชี ซึ่งจะต้องนำไปใช้ในการดำเนินงาน รวมทั้งจ่ายค่าธรรมเนียมธุรกรรมผ่านบัตรเครดิต ดังนั้นหาก Paypal จะทำกำไรได้มากก็จะต้องหวังว่าผู้ใช้เก็บเงินเอาไว้ในบัญชี Paypal แล้วนำไปใช้กับผู้ใช้คนอื่นต่อไปเรื่อยๆ

3.2 การควบคุมภายในของกิจการ

ระบบสารสนเทศทางการบัญชีเป็นระบบที่พัฒนาขึ้นมาในกิจการเพื่อนำข้อมูลที่ได้จากการปฏิบัติงานของหน่วยงานในองค์กร เช่น หน่วยงานด้านการตลาด หน่วยงานด้านการผลิต หน่วยงานด้านการเงิน และหน่วยงานด้านการบริหารทรัพยากรมนุษย์ มาจัดทำเป็นรายงานการเงินและรายงานเพื่อการบริหารส่งให้ผู้ใช้ทั้งภายในและภายนอก ผู้ใช้เหล่านี้ได้นำสารสนเทศในรายงานไปใช้ในการวิเคราะห์ ตัดสินใจ วางแผน และควบคุมการปฏิบัติงานของหน่วยงานที่รับผิดชอบ ดังนั้นสารสนเทศจึงต้องมีความถูกต้อง ครบถ้วน เชื่อถือได้ และทันเวลา ปัจจุบันนี้ได้มีการใช้การควบคุมภายใน (Internal Control) เป็นเครื่องมือควบคุมการปฏิบัติงานให้มีประสิทธิภาพ และมีระบบสารสนเทศที่ครบถ้วน ถูกต้อง และเชื่อถือได้

3.2.1 ความหมายของการควบคุมภายใน

การควบคุมภายใน หมายถึง กระบวนการปฏิบัติงานที่ผู้บริหารทุกระดับและพนักงานทุกคนในองค์กรกำหนดขึ้นเพื่อให้องค์กรบรรลุเป้าหมายที่สำคัญ 4 ประการคือ

- เพื่อดูแลรักษาทรัพย์สินและข้อมูลให้อยู่ในสถานที่ที่ปลอดภัย จากการทุจริตของผู้บริหาร พนักงาน หรือบุคคลภายนอก หากมีความเสียหายเกิดขึ้น การมีระบบควบคุมภายในที่ดีจะทำให้ทราบถึงความเสียหายนั้นเร็วที่สุด
- เพื่อให้มั่นใจว่าการจัดทำสารสนเทศทางการบัญชีมีความถูกต้อง เชื่อถือได้และนำเสนอได้ทันเวลา การมีระบบควบคุมภายในที่ดี จะทำให้ผู้ใช้ได้รับสารสนเทศที่ถูกต้อง และเชื่อถือได้ตรงตามเวลาที่กำหนด
- เพื่อสนับสนุนให้มีการปฏิบัติงานตามนโยบาย และข้อบังคับของกิจการหรือข้อกำหนดของกฎหมายอย่างต่อเนื่อง การมีระบบควบคุมภายในที่ดีจะป้องกันไม่ให้เกิดผลเสียหายจากการละเว้นการปฏิบัติงานตามนโยบาย และข้อบังคับของกิจการ หรือตามข้อกำหนดของกฎหมาย
- เพื่อส่งเสริมให้มีการปฏิบัติงานในองค์กรอย่างมีประสิทธิภาพ ระบบการควบคุมภายในที่ดีจะช่วยให้มีการใช้ทรัพยากรขององค์กร เช่น ทรัพยากรมนุษย์ ทรัพยากรทางการเงิน เวลา และทรัพย์สินอื่น อย่างมีประสิทธิภาพ ประหยัด และบรรลุเป้าหมายขององค์กร

การควบคุมภายในที่กำหนดให้มีกิจการนี้ไม่ได้เป็นสิ่งที่รับประกันหรือให้ความมั่นใจที่ทีสมบูรณ์ทั้ง 100% ว่า กิจการจะสามารถปฏิบัติงานจนบรรลุเป้าหมายที่ต้องการทั้ง 4 ประการ รวมทั้งไม่ได้รับประกันว่ากิจการจะไม่ประสบความล้มเหลวทางเศรษฐกิจเนื่องจากระบบการควบคุมภายในนั้นมีข้อจำกัดในการนำไปใช้ปฏิบัติงาน

3.2.2 การควบคุมภายในทางการบัญชี (Accounting Control)

ประกอบด้วยแผนการจัดแบ่งส่วนงาน วิธีการ และการจดบันทึกรายการค้า เพื่อวัตถุประสงค์จะดูแลรักษาทรัพย์สิน และมีการบันทึกบัญชีที่ถูกต้องและเชื่อถือได้ มีเนื้อหาดังนี้

- การอนุมัติรายการ (Authorization or Approval) รายการค้าทุกรายการจะต้องผ่านการอนุมัติโดย ผู้บริหาร
- ความถูกต้องของรายการ (Validity) รายการค้าที่นำมาบันทึกบัญชีจะต้องเป็นรายการค้าที่เกิดขึ้นจริงสำหรับกิจการนั้นๆ
- มีความครบถ้วน (Completeness) รายการค้าที่ได้รับอนุมัติจะต้องนำมาบันทึกบัญชีโดยครบถ้วนทุกรายการ
- ความถูกต้องในการบันทึกบัญชี (Recording Accuracy) รายการค้าจะต้องนำมาบันทึกบัญชีโดยถูกต้อง ทั้งประเภทบัญชี จำนวนเงิน งวดบัญชี
- การเก็บรักษาทรัพย์สิน (Safe Guarding) ต้องมีการกำหนดผู้รับผิดชอบดูแลรักษาทรัพย์สิน ซึ่งต้องไม่ใช่ผู้มีหน้าที่บันทึกบัญชีและอนุมัติรายการ
- การพิสูจน์ยอด (Reconciliation) ต้องมีการเปรียบเทียบรายการในบัญชีกับรายละเอียด ถ้ามีข้อแตกต่างต้องหาคำอธิบายจนเป็นที่พอใจ และอาจมีรายการปรับปรุงที่จำเป็น

3.2.3 การควบคุมภายในของกระบวนการสับเปลี่ยนข้อมูลอิเล็กทรอนิกส์

เนื่องจากกระบวนการสับเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์เป็นกระบวนการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์ของคู่ค้าทำให้ไม่มีเอกสารทางธุรกิจที่จัดพิมพ์ลงบนแผ่นกระดาษเพื่อใช้เป็นหลักฐานในการบันทึกบัญชี และหลักฐานการตรวจสอบ (audit trail) ดังนั้น เพื่อให้ผู้ใช้สารสนเทศทางการบัญชีมั่นใจว่า รายการค้าที่เกิดขึ้นในกระบวนการสับเปลี่ยนข้อมูลอิเล็กทรอนิกส์มีความถูกต้อง ครบถ้วน เชื่อถือได้ ปลอดภัยจากการบุกรุกของผู้ที่ไม่ได้รับอนุญาตให้เข้าถึง (access) ข้อมูล รวมทั้ง มีการบันทึกรายการที่เกิดขึ้นระหว่างการปฏิบัติงานอยู่ตลอดเวลา กิจการจึงต้องมีระบบการควบคุมภายในที่มีประสิทธิภาพและประเมินประสิทธิภาพของการควบคุมภายในอยู่เป็นระยะ โดยเฉพาะในเรื่องของความเชื่อถือได้ของข้อมูล และการรักษาความปลอดภัยของข้อมูลนั้นควรกำหนดให้มีการควบคุมภายในขั้นพื้นฐานเพิ่มเติมดังนี้

- กำหนดให้มีการเข้ารหัสลับ (Data Encryption) ด้วยวิธีการใช้รหัสผ่าน (password หรือ digital key) เพื่อเปลี่ยนข้อความต้นฉบับ (readable/plaintext message) ให้กลายเป็นข้อความที่เข้ารหัส (ciphertext message) ซึ่งบุคคลทั่วไปอ่านแล้วไม่เข้าใจ แต่ผู้รับที่เป็นลูกค้าซึ่งทราบรหัสลับ (secret key cryptography) สามารถแปลงข้อความที่เข้ารหัสมา

เป็นข้อความต้นฉบับได้ วิธีการเข้ารหัสลับนี้ สามารถป้องกันไม่ให้บุคคลอื่นนอกจากลูกค้าลักลอบเข้ามาขโมย แก้ไขข้อมูล และทำรายการปลอมในระบบได้

- กำหนดให้มีตัวป้องกันการบุกรุก (Firewalls) โดยกำหนดให้มีจุดเชื่อมการส่ง หรือการรับข้อมูลระหว่างเครือข่ายภายนอกซึ่งเป็นอินเตอร์เน็ตกับเครือข่ายภายในกิจการซึ่งเป็นอินทราเน็ตที่แน่นอนเพียงจุดเดียว เพื่อป้องกันไม่ให้บุคคลภายนอกที่ไม่มีสิทธิ (unwarranted intrusion from external parties) สามารถบุกรุกเข้ามาดูข้อมูลในกลุ่มข้อมูล (packet) ที่ส่งผ่านระหว่างอุปกรณ์สื่อสาร หรือระหว่างผู้รับกับผู้ส่งข้อมูลที่อยู่ในเครือข่ายคอมพิวเตอร์
- กำหนดให้มีตัวบริการแทน (Proxy Servers) ทำหน้าที่เป็นตัวแทนรับข้อมูลจากเครือข่ายอินเตอร์เน็ต เพื่อการสอบสิทธิของผู้รับ-ส่งข้อมูล รวมทั้งความปลอดภัยของข้อมูลก่อนที่จะส่งต่อไปยังเครื่องคอมพิวเตอร์ภายในเครือข่ายของกิจการที่เกี่ยวข้อง วิธีนี้สามารถป้องกันการใช้ระบบโดยไม่มีสิทธิ รวมทั้งสามารถกลั่นกรองข้อมูลการติดต่อจากเครือข่ายภายนอกกิจการได้
- กำหนดระดับขั้นของการเข้าถึงแฟ้มข้อมูล (Degree of Access) เนื่องจากการสื่อสารในระบบนี้ได้เปิดโอกาสให้บริษัทผู้ซื้อสามารถเข้าถึงข้อมูลในแฟ้มข้อมูลสินค้าคงคลังของผู้ขายเพื่อดูระดับคงเหลือของสินค้าคงคลังว่ามีจำนวนเพียงพอที่จะสั่งซื้อหรือไม่ และผู้ซื้อยังสามารถเข้าถึงข้อมูลราคาขายของสินค้าแต่ละประเภทของผู้ขายเพื่อนำมาใช้ประกอบการตัดสินใจสั่งซื้ออีกด้วย ดังนั้นเพื่อป้องกันไม่ให้ผู้ซื้อสามารถเข้าไปเปลี่ยนแปลงแก้ไขข้อมูลในแฟ้มข้อมูลของผู้ขายได้ ผู้ขายจึงควรกำหนดขั้นของการเข้าถึงแฟ้มข้อมูล เช่น กำหนดให้ผู้ซื้อสามารถเข้าถึงข้อมูลเกี่ยวกับจำนวนคงเหลือและราคาขายของสินค้าคงเหลือแต่ละประเภทได้เพียงอย่างเดียว แต่ไม่สามารถเปลี่ยนแปลงตัวเลขได้ เป็นต้น

กำหนดให้มีการบันทึกข้อมูลการปฏิบัติงานลงในแฟ้มข้อมูลบันทึกการปฏิบัติงาน ทุกครั้งที่เกิดรายการค้าเพื่อที่นักบัญชี และผู้สอบบัญชีสามารถใช้เป็นหลักฐานในการตรวจสอบความถูกต้อง ความสมบูรณ์ ความครบถ้วน และระยะเวลาที่เกิดรายการค้าได้ เช่นเดียวกับการติดต่อค้าขายกันด้วยเอกสารที่จัดพิมพ์ลงบนแผ่นกระดาษ กระบวนการบันทึกข้อมูลการปฏิบัติงานของบริษัทผู้ซื้อจะเริ่มขึ้นเมื่อมีการส่งข้อมูลการจัดซื้อในรูปแบบของเอกสารอิเล็กทรอนิกส์ ผ่านตู้ไปรษณีย์อิเล็กทรอนิกส์ของบริษัทผู้ซื้อไปยังตู้ไปรษณีย์อิเล็กทรอนิกส์ของผู้ขาย ซึ่งเรียกธุรกรรมส่วนนี้ว่า ส่วนของลูกค้า และส่วนของกิจการจะเกิดขึ้นหลังจากที่ระบบการสั่งขายของบริษัทผู้ขายรับทราบข้อมูลการสั่งซื้อ กิจการส่วนหน้า (Front office) ก็จะบันทึกข้อมูลการสั่งซื้อลงในแฟ้มข้อมูลบันทึกการปฏิบัติงาน และส่งข้อมูลการสั่งซื้อต่อมายังกิจการส่วนหลัง (Back office) เพื่อดำเนินการต่อไป เมื่อบริษัทผู้ขายอนุมัติการขาย

รวมทั้ง แจ้งข้อมูลการขาย และข้อมูลการส่งสินค้าไปยังบริษัทผู้ซื้อ ชุดคำสั่งงานของบริษัทผู้ขายก็จะบันทึกข้อมูลดังกล่าวลงในแฟ้มข้อมูลบันทึกการปฏิบัติงาน ในด้านบริษัทผู้ซื้อนั้น เมื่อได้รับแจ้งข้อมูลการขายสินค้า และข้อมูลการส่งสินค้าจากบริษัทผู้ขายก็จะบันทึกข้อมูลลงในแฟ้มข้อมูลบันทึกการปฏิบัติงาน เช่นกัน

3.3 ระบบความปลอดภัยบนอินเตอร์เน็ต

เนื่องจากไม่มีเทคโนโลยีใดที่จะมีความปลอดภัยร้อยเปอร์เซ็นต์ เพราะเทคโนโลยีทั้งหมดสร้างขึ้นโดยมนุษย์ ดังนั้นย่อมที่จะรู้และเข้าใจ จนมีผู้ที่สามารถทะลุทะลวงระบบรักษาความปลอดภัยได้ ดังเช่นที่พบเห็นและเป็นข่าวอยู่เสมอเกี่ยวกับกลุ่มแฮกเกอร์เข้าบุกทำลายระบบต่าง ๆ แม้ว่าระบบเหล่านั้นจะได้รับการออกแบบมาอย่างดีแล้วก็ตาม

3.2.1 ประเภทของระบบความปลอดภัยของข้อมูล

ความปลอดภัยสำหรับการใช้ และการทำพาณิชย์อิเล็กทรอนิกส์ สามารถแบ่งออกเป็น 2 ส่วน คือ ความปลอดภัยทางกายภาพ (Physical Security) และความปลอดภัยของข้อมูล (Information Security) ซึ่งมักจะเน้นที่ความปลอดภัยของข้อมูลเป็นหลัก เนื่องจากข้อมูลเป็นสิ่งที่อาจจะถือได้ว่าเป็นหัวใจในการทำธุรกิจก็ว่าได้ และง่ายต่อการถูกคุกคาม เพราะพาณิชย์อิเล็กทรอนิกส์นั้นจะเป็นการรับส่งหรือแลกเปลี่ยนข้อมูลกันบนเครือข่าย ซึ่งข้อมูลที่กล่าวถึงจะอยู่ในทุก ๆ ส่วนของธุรกรรมพาณิชย์อิเล็กทรอนิกส์ที่เดียว ไม่ว่าจะเป็นการค้นหาข้อมูล การโฆษณา การสั่งซื้อ การชำระเงิน และการส่งสินค้า หรือบริการ ระบบรักษาความปลอดภัยของข้อมูลของพาณิชย์อิเล็กทรอนิกส์จึงต้องมีมาตรการดังต่อไปนี้

- การระบุตัวบุคคล และอำนาจหน้าที่ (Authentication & Autorization) คือ การระบุตัวบุคคลที่ติดต่อว่าเป็นบุคคลตามที่ได้กล่าวอ้างไว้จริง และมีอำนาจหน้าที่ตามที่ได้กล่าวอ้างไว้จริง
- การรักษาความลับของข้อมูล (Confidentiality) คือ การรักษาความลับของข้อมูลที่เก็บไว้หรือส่งผ่านทางเครือข่าย โดยป้องกันไม่ให้ผู้อื่นที่ไม่มีสิทธิ์ลักลอบดูได้
- การรักษาความถูกต้องของข้อมูล (Integrity) คือ การป้องกันไม่ให้ข้อมูลถูกแก้ไข โดยตรวจสอบไม่ได้
- การป้องกันการปฏิเสธ หรืออ้างความรับผิดชอบ (Non-repudiation) คือ การป้องกันการปฏิเสธว่าไม่ได้มีการส่ง หรือรับข้อมูล จากฝ่ายต่าง ๆ ที่เกี่ยวข้อง หรือการป้องกันการอ้างที่เป็นเท็จได้รับ-ส่งข้อมูล
- ลายมือชื่อดิจิตอล (Digital Signature) คือ ข้อมูลอิเล็กทรอนิกส์ที่ได้จากการเข้ารหัสข้อมูลด้วยกุญแจส่วนตัวของผู้ส่งซึ่งเปรียบเสมือนเป็นลายมือของผู้ส่ง คุณสมบัติของลายมือชื่อ

ดิจิตอลนอกจากจะสามารถระบุตัวบุคคล และเป็นกลไกการป้องกันการปฏิเสธความรับผิดชอบแล้ว ยังสามารถป้องกันข้อมูลที่ส่งไปไม่ให้ถูกแก้ไข หรือหากถูกแก้ไขไปจากเดิมก็ไม่สามารถล่วงรู้ได้

3.2.2 ปัญหาหลักในเรื่องระบบรักษาความปลอดภัย

ปัญหาหลักของระบบรักษาความปลอดภัยไม่ได้อยู่ที่เทคโนโลยี ทั้งนี้เพราะเทคโนโลยีสร้างขึ้นมาเพื่อป้องกัน และเปิดโอกาสให้ผู้มีสิทธิ์ใช้งานได้ตามต้องการ ปัญหาอยู่ที่การจัดการสิทธิ และหน้าที่ของแต่ละบุคคลที่เกี่ยวข้องกับระบบ

จากการสำรวจเกี่ยวกับพาณิชย์อิเล็กทรอนิกส์ของหลาย ๆ แหล่งรวมทั้งการสำรวจของศูนย์พาณิชย์อิเล็กทรอนิกส์พบว่าประเด็นหลักใหญ่ที่สุดที่เป็นอุปสรรคของการพัฒนาพาณิชย์อิเล็กทรอนิกส์ได้แก่ ความปลอดภัยสำหรับการใช้ และการทำพาณิชย์อิเล็กทรอนิกส์

ตัวอย่างการคุกคามทางอินเตอร์เน็ต ได้แก่

- การเข้าถึงระบบเครือข่ายของผู้ที่ไม่มีสิทธิ์
- การเข้ามาทำลาย เปลี่ยนแปลง หรือขโมยข้อมูล
- การนำข้อมูลไปเปิดเผยยังผู้ไม่มีสิทธิ์
- การทำให้การทำงานของระบบหยุดชะงัก
- การปฏิเสธความรับผิดชอบในการทำธุรกรรม หรือการอ้างว่าได้รับ หรือ ให้บริการ/ข้อมูลของผู้ซื้อ หรือผู้ขาย ซึ่งถ้าข้อมูลเหล่านั้นเกี่ยวข้องกับ ข้อมูลทางการเงิน เช่น หมายเลขบัตรเครดิต ข้อมูลลับของบริษัท (Corporate Secret) หรือข้อมูลที่เป็นทรัพย์สินทางปัญญา (Proprietary Information) จะก่อให้เกิดความเสียหายอย่างมาก

3.2.3 นโยบายของรัฐกับมาตรการรักษาความปลอดภัย

ประเทศไทยจำเป็นต้องก้าวเข้าสู่การใช้ประโยชน์จากเครือข่าย และไอทีให้มาก การสร้างความเชื่อมั่นในระบบธุรกิจนั้นดำเนินไปได้ หากเรียกความเชื่อมั่นไม่ได้นั้นก็ยากที่จะประสบความสำเร็จ ยิ่งในปัจจุบันหลายธนาคารในประเทศไทยกำลังเปิดบริการบนอินเตอร์เน็ต เพื่อให้ชำระเงินผ่านทางอินเตอร์เนตได้ ความสำเร็จของธุรกิจจึงอยู่ที่ความมั่นใจ ความเชื่อถือ

สำนักงานตำรวจแห่งชาติจึงต้องปรับตัวเอง โดยเฉพาะการเตรียมบุคลากรที่สามารถจับผู้กระทำผิด ตรวจเฝ้ามอง และดูแลความสงบสุขในการใช้ไอที ภาระหน้าที่นี้เป็นส่วน ช่วยส่งเสริมธุรกิจการค้า และพาณิชย์อิเล็กทรอนิกส์ในประเทศไทยให้ขยายตัวได้ เพราะหนทางบนอินเตอร์เน็ตเป็นที่สาธารณะที่มิจฉาชีพอาจแฝงตัวได้ง่าย ระบบเฝ้ามองจึงต้องได้รับการกำหนดอย่างเป็นรูปธรรมเมื่อมี

การเฝ้าระวังแล้ว จำเป็นต้องมีการพัฒนากฎหมายต่าง ๆ สร้างระบบลงโทษผู้กระทำผิดอย่างเป็นรูปธรรมอีกด้วย

ปัจจุบันในส่วนของรัฐบาลได้มีการออกร่างพระราชบัญญัติการพาณิชย์ทางอิเล็กทรอนิกส์ซึ่งจะแสดงไว้ในส่วนของภาคผนวก ก.