

2

การกำกับดูแลเสถียรภาพระบบการชำระเงิน (Payment Systems Stability)

2.1 บทบาทหน้าที่ของ ธปท. ในการกำกับดูแลระบบการชำระเงินที่สำคัญ

ระบบการชำระเงินเป็นโครงสร้างพื้นฐานทางการเงินที่มีความสำคัญอย่างยิ่งต่อการหมุนเวียนเงินและการเติบโตของระบบเศรษฐกิจของประเทศ โดยช่วยสนับสนุนและรองรับการทำธุรกรรมทางการเงินของสถาบันการเงินภาครัฐ ภาคเอกชน รวมถึงกลุ่มธุรกิจรายย่อย และประชาชนทั่วไป จึงควรมีการกำกับดูแลให้ระบบการชำระเงินมีการบริหารจัดการที่ดี มีความปลอดภัย สามารถให้บริการได้อย่างต่อเนื่อง รวมทั้งมีการคุ้มครองผู้บริโภคอย่างเหมาะสม เพื่อสร้างความเชื่อมั่นในการใช้บริการด้วย

ธปท. มีหน้าที่ในการดูแลเสถียรภาพระบบการชำระเงินของประเทศให้มีการดำเนินการอย่างมีประสิทธิภาพ มีความปลอดภัย มีการคุ้มครองผู้บริโภค มีการบริหารจัดการความเสี่ยงที่เหมาะสม รวมถึงการดำเนินการที่สอดคล้องตามมาตรฐานสากล Principles for Financial Market Infrastructures (PFMIs) ของ Bank for International Settlements (BIS) โดยในการกำกับดูแลดังกล่าว มีหน่วยงานและคณะกรรมการที่เกี่ยวข้อง ได้แก่ คณะกรรมการระบบการชำระเงิน (กรช.) เป็นผู้กำหนดนโยบายการกำกับดูแลระบบการชำระเงินที่มีความสำคัญ รวมทั้งการดูแลเสถียรภาพระบบการชำระเงินของประเทศ และคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (ครอ.) เป็นผู้กำหนดนโยบายการกำกับดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

2.2 ระบบการชำระเงินที่มีความสำคัญ

ระบบการชำระเงินที่มีความสำคัญที่ ธปท. กำกับดูแล จำแนกเป็น 2 ประเภท ดังนี้

- 1) ระบบการชำระเงินที่สำคัญต่อความมั่นคงของระบบการเงินของประเทศ (Systemically Important Payment System: SIPS) ซึ่งเป็นโครงสร้างพื้นฐานรองรับการโอนเงินหรือการชำระเงินมูลค่าสูงระหว่างสถาบัน ซึ่งมีเพียงระบบเดียวในประเทศไทย คือ ระบบบาทเน็ต (Bank of Thailand Automated High-value Transfer Network: BAHTNET) ที่ดำเนินการโดย ธปท.
- 2) ระบบการชำระเงินรายย่อยที่มีความสำคัญ (Prominently Important Retail Payment Systems: PIRPS) ได้แก่ ระบบการหักบัญชีเช็คด้วยภาพเช็ค (Imaged Cheque Clearing and Archive System: ICAS) ซึ่งดำเนินการโดย ธปท. และระบบการโอนเงินรายย่อยระหว่างธนาคาร เช่น ระบบ ATM Pool และระบบการโอนเงินรายย่อยระหว่างธนาคารครั้งละหลายรายการ (bulk payment) ซึ่งดำเนินการโดยบริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด (NITMX)

2.3 วิธีการกำกับดูแลระบบการชำระเงินที่มีความสำคัญ (Oversight Approach)

ธปท. กำหนดวิธีการกำกับดูแลระบบการชำระเงินที่มีความสำคัญไว้ในนโยบายการกำกับดูแลระบบการชำระเงินที่สำคัญ (Oversight Policy Framework) ดังนี้

- 1) การจัดให้มีการวิเคราะห์ ติดตาม และประเมินความเสี่ยงของระบบการชำระเงินที่สำคัญเป็นระยะ เพื่อประเมินผลกระทบที่เกิดจากความเสี่ยงที่สำคัญ เช่น ความเสี่ยงด้านสภาพคล่อง (liquidity risk) ความเสี่ยงด้านปฏิบัติการ (operational risk) และความเสี่ยงในการชำระดุล (settlement risk) รวมทั้งความเสี่ยงต่อระบบ (systemic risk) ในกรณีที่เกิดเหตุการณ์ต่าง ๆ ที่ไม่ปกติ หรือเหตุวิกฤติ รวมถึงผลกระทบในกรณีที่มีการเปลี่ยนแปลงระบบหรือหลักเกณฑ์ที่สำคัญของระบบ
- 2) การกำหนดให้ผู้ดำเนินการระบบจัดทำประเมินระบบด้วยตนเอง (self-assessment) โดยอ้างอิงตามมาตรฐานสากล PFMI
- 3) การเข้าประเมินและสังเกตการณ์การปฏิบัติงานของผู้ให้บริการระบบ เพื่อมุ่งเน้นการประเมินความเสี่ยงที่อาจเกิดขึ้นในขั้นตอนการปฏิบัติงานและระบบให้บริการ

นอกจากนี้ ธปท. ได้ร่วมมือและประสานงานเพื่อการกำกับดูแล (cooperative oversight) กับสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)⁶ โดยได้แลกเปลี่ยนข้อมูลเกี่ยวกับการกำกับดูแลระบบโครงสร้างพื้นฐานทางการเงิน (Financial Market Infrastructures: FMIs) และความคืบหน้าในการกำกับดูแลระบบที่เชื่อมโยงกัน ตลอดจนการกำหนดหลักเกณฑ์ และมาตรการจัดการความเสี่ยงในระบบที่สอดคล้องกัน เพื่อให้ระบบ FMIs มีการดำเนินการโดยสอดคล้องกับมาตรฐานสากล PFMI

2.4 การดูแลเสถียรภาพระบบการชำระเงินที่สำคัญ

2.4.1 ระบบบาทเน็ต (Bank of Thailand Automated High-Value Transfer Network: BAHTNET)

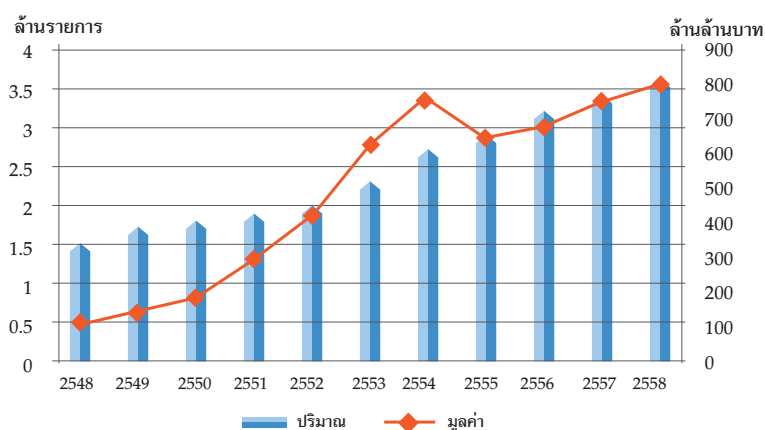
เป็นระบบการโอนเงินมูลค่าสูงที่มีความสำคัญ รองรับการทำธุรกรรมการโอนเงินระหว่างสถาบันที่มีบัญชีเงินฝากกับ ธปท. เช่น การโอนเงินระหว่างสถาบัน การโอนเงินเพื่อบุคคลที่สาม การโอนเงินเพื่อชำระราคาหลักทรัพย์ และการชำระดุลสุทธิพร้อมกันหลายฝ่าย ธปท. จึงต้องมีการกำกับดูแลให้สอดคล้องตามมาตรฐานสากล PFMI เพื่อให้ระบบบาทเน็ตมีการดำเนินการและบริหารจัดการความเสี่ยงอย่างเหมาะสมและสามารถให้บริการได้อย่างต่อเนื่อง ทั้งภาวะปกติและภาวะฉุกเฉิน



⁶ ก.ล.ต. กำกับดูแลระบบการชำระราคาและส่งมอบหลักทรัพย์ (Securities Settlement System: SSS) ระบบสำนักหักบัญชีกลางสำหรับธุรกรรมการซื้อขายหลักทรัพย์ (Central Counterparties: CCP) ซึ่งดำเนินการโดยบริษัท สำนักหักบัญชี (ประเทศไทย) จำกัด (Thailand Clearing House: TCH) และระบบศูนย์รับฝากหลักทรัพย์ (Central Securities Depositories: CSD) ของบริษัท ศูนย์รับฝากหลักทรัพย์ (ประเทศไทย) จำกัด (Thailand Securities Depository: TSD)

ในปี 2558 การโอนเงินผ่านระบบบาทเน็ตมีปริมาณทั้งสิ้น 3.6 ล้านรายการ คิดเป็นมูลค่า 790 ล้านล้านบาท โดยมีปริมาณเพิ่มขึ้นจากปี 2557 ร้อยละ 6.4 และมูลค่าเพิ่มขึ้นร้อยละ 4.3 สำหรับปริมาณและมูลค่าการโอนเงินผ่านระบบบาทเน็ตมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง โดยมีจำนวนรายการเฉลี่ยต่อวันอยู่ที่ 14,800 รายการ และมีมูลค่าเฉลี่ยต่อวันอยู่ที่ 3.3 ล้านล้านบาท ทั้งนี้มีมูลค่าการโอนเงินผ่านระบบบาทเน็ตคิดเป็น 58.4 เท่าของ GDP

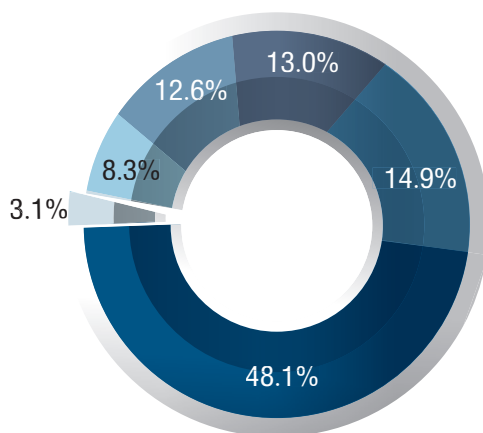
ภาพที่ 3 : ปริมาณและมูลค่าการโอนเงินผ่านระบบบาทเน็ต



ที่มา: ธนาคารแห่งประเทศไทย

สำหรับการโอนเงินผ่านระบบบาทเน็ตแยกตามประเภทธุรกิจ พบว่าธุรกรรมซื้อคืนพันธบัตรแบบทวิภาคี (Bilateral repurchase operations: Bilateral RP) คิดเป็นสัดส่วนสูงสุดถึงร้อยละ 48.1 มีมูลค่า 375.7 ล้านล้านบาท รองลงมาได้แก่ ธุรกรรมโอนเงินระหว่างสถาบัน (ร้อยละ 14.9) การซื้อขายหลักทรัพย์ (ร้อยละ 13.0) การโอนเงินภายในสถาบันเดียวกัน (ร้อยละ 12.6) การซื้อขายเงินตราต่างประเทศ (ร้อยละ 8.3) และธุรกรรมกู้ยืมเงินระหว่างสถาบัน (ร้อยละ 3.1)

ภาพที่ 4 : สัดส่วนมูลค่าการโอนเงินผ่านระบบบาทเน็ตแยกตามประเภทธุรกรรมที่สำคัญ



- ธุรกรรมกู้ยืมเงินระหว่างสถาบัน
- ธุรกรรมซื้อขายเงินตราต่างประเทศ
- การโอนเงินภายในสถาบันเดียวกัน
- ธุรกรรมซื้อขายหลักทรัพย์
- การโอนเงินระหว่างสถาบัน
- อื่น ๆ (รวม Bilateral RP)

ที่มา: ธนาคารแห่งประเทศไทย

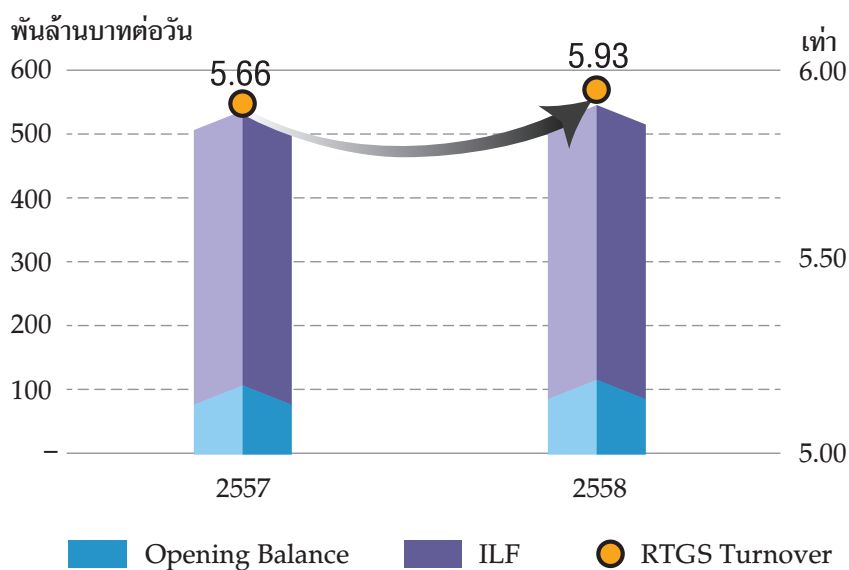
- การบริหารจัดการความเสี่ยงที่สำคัญของระบบบาทเนต

(1) การบริหารจัดการความเสี่ยงด้านสภาพคล่องและความเสี่ยงในการชำระดุล

สมาชิกของระบบบาทเนตมีสภาพคล่องเพียงพอสำหรับทำรายการโอนเงินผ่านระบบบาทเนต และยังไม่ประสบปัญหาความเสี่ยงในการชำระดุล (settlement risk) โดยในปี 2558 สมาชิกมีสภาพคล่องระหว่างวันซึ่งประกอบด้วย เงินฝากของสมาชิกผู้ใช้บริการในบัญชีที่ ธปท. (Opening Balance) และเงินสภาพคล่องระหว่างสถาบันที่สมาชิกได้รับจาก ธปท. โดยมีหลักทรัพย์ค้ำประกัน (Intraday Liquidity Facility: ILF) เฉลี่ยเท่ากับ 548.7 พันล้านบาทต่อวัน เพิ่มขึ้นจากปี 2557 ร้อยละ 0.3 หรือเพิ่มขึ้น 1.8 พันล้านบาทต่อวัน เมื่อพิจารณาอัตราการหมุนเวียนของสภาพคล่องเพื่อใช้ในการโอนเงินผ่านระบบบาทเนต (RTGS Turnover) ในแต่ละวันพบว่า มีค่าเท่ากับ 5.7 เท่า ในปี 2557 และ 5.9 เท่า ในปี 2558 นอกจากนี้ รายการโอนเงินที่รอสภาพคล่อง (รายการค้างคิวในระบบบาทเนต) มีเพียงร้อยละ 1.5 ของปริมาณธุรกรรมโอนเงินทั้งหมด

ในส่วนของการดูแลความเสี่ยงด้านการชำระดุลหลายฝ่าย (Multilateral Net Settlement) ธปท. ได้จัดให้มีมาตรการ Securities Requirement for Settlement (SRS) เริ่มบังคับใช้เมื่อ 2 กรกฎาคม 2558 โดยกำหนดให้ธนาคารสมาชิกวางหลักประกันเพื่อรองรับความเสี่ยงจากการชำระดุลที่เป็น net settlement เช่น การชำระดุลจากการหักบัญชี เช็ค การโอนเงินรายย่อยระหว่างธนาคาร เป็นต้น ในอัตราไม่น้อยกว่าฐานะขาดดุลสูงสุดที่อาจเกิดขึ้น เพื่อลดความเสี่ยงหากสมาชิกรายใดรายหนึ่งมีเงินไม่เพียงพอที่จะชำระดุลและอาจมีผลกระทบต่อสมาชิกรายอื่น ๆ ในระบบ ซึ่งที่ผ่านมาการชำระดุลสามารถดำเนินการสำเร็จลุล่วงตามเวลาที่กำหนดโดยไม่ต้องบังคับใช้หลักประกัน SRS แต่อย่างใด

ภาพที่ 5 : สภาพคล่องระหว่างวันโดยเฉลี่ยของระบบบาทเนต



ที่มา: ธนาคารแห่งประเทศไทย

(2) การบริหารจัดการความเสี่ยงด้านปฏิบัติการ (Operational Risk)

ความเสี่ยงด้านปฏิบัติการเป็นความเสี่ยงที่สำคัญของระบบบาทเน็ต ซึ่ง ธปท. ต้องดูแลให้ระบบสามารถดำเนินการได้อย่างต่อเนื่องทั้งภาวะปกติและภาวะฉุกเฉิน การบริหารจัดการความต่อเนื่องระบบบาทเน็ต เป็นส่วนสำคัญที่สนับสนุนให้ระบบการชำระเงินเป็นไปอย่างราบรื่น ธปท. ในฐานะผู้ให้บริการระบบบาทเน็ต ได้กำหนดตัวชี้วัดความต่อเนื่องของบริการ (target system availability) ที่ร้อยละ 99.7 จากการดำเนินงานที่ผ่านมา ในปี 2558 ตัวชี้วัดความต่อเนื่องของบริการ (system availability) ของระบบบาทเน็ต เท่ากับ 99.95% ซึ่งอยู่ในระดับที่สูงกว่าเป้าหมายที่กำหนดไว้ โดย ธปท. มีการติดตามตัวชี้วัดความต่อเนื่องของบริการของระบบบาทเน็ต และรายงานต่อผู้บริหารที่เกี่ยวข้อง รวมทั้งรายงานผลการดำเนินการต่อ กรช. เป็นประจำทุก 6 เดือน

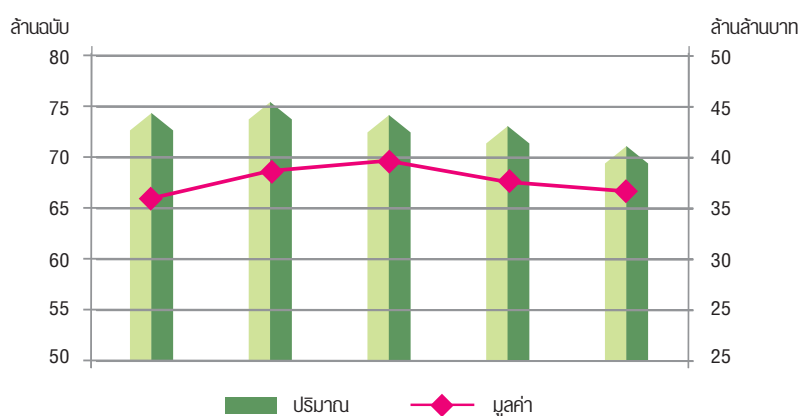
• การกำกับดูแลระบบบาทเน็ตตามมาตรฐาน PFMI

ธปท. มีการเตรียมความพร้อมด้านระบบการชำระเงินเพื่อเข้ารับการประเมินตามโครงการ Financial Sector Assessment Program (FSAP) โดยในปี 2558 – 2559 ธปท. ได้ดำเนินการเพื่อให้ระบบบาทเน็ตมีการบริหารจัดการอย่างมีประสิทธิภาพและสอดคล้องตามมาตรฐานสากลมากยิ่งขึ้น ได้แก่ เร่งผลักดันให้มีกฎหมายรองรับ payment finality และการจัดให้มีพิธีปฏิบัติและกระบวนการจัดการเมื่อสมาชิกในระบบเกิดปัญหาไม่สามารถชำระดุลได้หรือล้มละลาย (default management) รวมทั้งการจัดทำกรอบนโยบายการจัดการความเสี่ยงของระบบบาทเน็ต (risk management framework) เพื่อให้สอดคล้องกับมาตรฐาน PFMI

2.4.2 ระบบการหักบัญชีเช็คด้วยภาพเช็ค (Imaged Cheque Clearing and Archive System: ICAS)

ICAS เป็นระบบการชำระเงินรายย่อยที่มีความสำคัญที่รองรับการเรียกเก็บเช็คด้วยภาพเช็คระหว่างธนาคาร ซึ่ง ธปท. ได้กำกับดูแลให้สอดคล้องตามมาตรฐานสากล PFMI โดยนำ PFMI ที่เกี่ยวข้องกับระบบการชำระเงินรายย่อยมาประยุกต์ใช้ จำนวน 14 ข้อ จากทั้งหมด 18 ข้อ

ภาพที่ 6 : ปริมาณและมูลค่าเช็คเรียกเก็บระหว่างธนาคารทั่วประเทศ

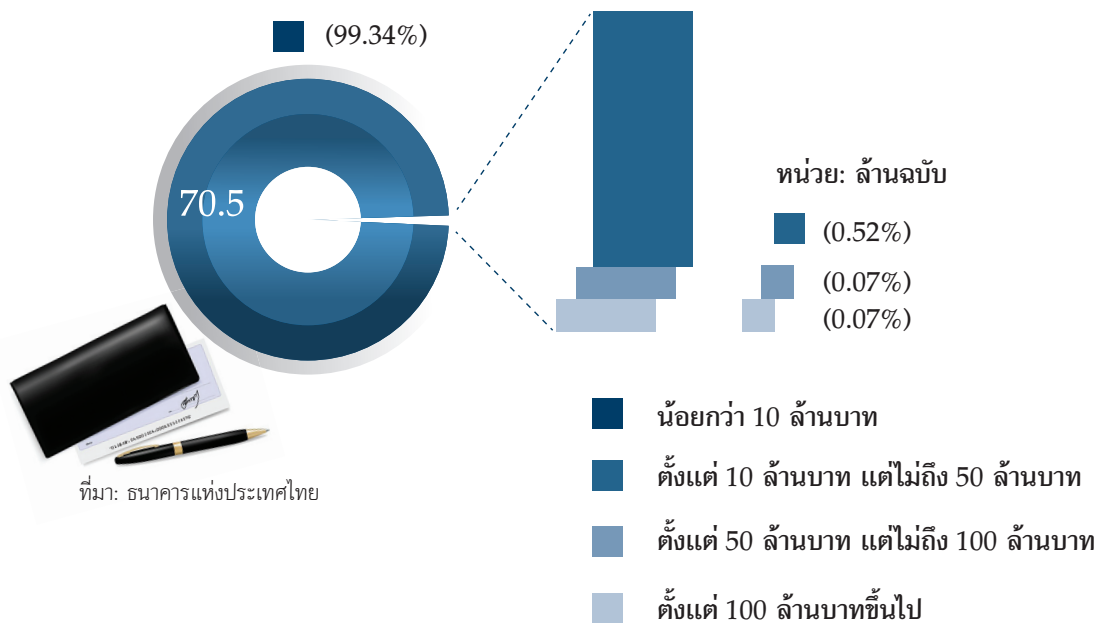


ที่มา: ธนาคารแห่งประเทศไทย

ในปี 2558 เช็ครีเอกเก็บระหว่างธนาคารทั่วประเทศ มีจำนวนทั้งสิ้น 71.0 ล้านฉบับ คิดเป็นมูลค่า 37.4 ล้านล้านบาท ลดลงจากปี 2557 ร้อยละ 2.3 และ 1.4 ตามลำดับ โดยปริมาณและมูลค่าเช็ครีเอกเก็บเฉลี่ยต่อวันอยู่ที่ 292,331 ฉบับ หรือ 154.1 พันล้านบาท ซึ่งมีแนวโน้มลดลงเช่นกันเนื่องจากสภาวะเศรษฐกิจในประเทศและแนวโน้มของการทำธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ที่เพิ่มมากขึ้นในช่วงระยะหลายปีที่ผ่านมา

ในปี 2558 เขตกรุงเทพและปริมณฑลมีสัดส่วนของปริมาณการเรียกเก็บเช็คในช่วงมูลค่าน้อยกว่า 10 ล้านบาท อยู่ในสัดส่วนมากที่สุดถึงร้อยละ 99.3 หรือประมาณ 70.5 ล้านฉบับ อันดับรองลงมาคือ เช็คมูลค่าตั้งแต่ 10 ล้านบาท แต่ไม่ถึง 50 ล้านบาท (ร้อยละ 0.52) เช็คมูลค่าตั้งแต่ 50 ล้านบาท แต่ไม่ถึง 100 ล้านบาท (ร้อยละ 0.07) และ มูลค่าตั้งแต่ 100 ล้านบาทขึ้นไป (ร้อยละ 0.07)

ภาพที่ 7: ปริมาณการเรียกเก็บเช็คในกรุงเทพและปริมณฑล แยกตามมูลค่า ปี 2558



• การบริหารจัดการความเสี่ยงที่สำคัญของระบบ ICAS

รพท. มีการบริหารจัดการความเสี่ยงด้านปฏิบัติการและการบริหารจัดการความต่อเนื่องของระบบ ICAS มาอย่างต่อเนื่อง ซึ่งได้กำหนดเป้าหมายตัวชี้วัดความต่อเนื่องของบริการที่ร้อยละ 99.7 จากการดำเนินงานที่ผ่านมาในปี 2558 ตัวชี้วัดความต่อเนื่องของบริการของระบบ ICAS เท่ากับร้อยละ 99.99 ซึ่งอยู่ในระดับที่สูงกว่าเป้าหมายที่กำหนดไว้ โดย รพท. ติดตามตัวชี้วัดความต่อเนื่องของบริการของระบบ ICAS และรายงานต่อผู้บริหารที่เกี่ยวข้อง รวมทั้งรายงานผลการดำเนินการต่อ กรช. เป็นประจำทุก 6 เดือน



• การกำกับดูแลระบบ ICAS

สปท. ได้นำมาตรฐานสากล PFMIIs มาประยุกต์ใช้ในการกำกับดูแลระบบ ICAS โดยในปี 2558 สปท. ได้ประเมินระบบ ICAS ในลักษณะ onsite examination เกี่ยวกับความเสี่ยงด้านปฏิบัติการ (หลักการข้อ 17: Operational risk) ใน 2 เรื่อง ได้แก่ (1) ความน่าเชื่อถือด้านการปฏิบัติงาน (Operational reliability and availability) และ (2) การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) โดยผลการประเมินสรุปได้ว่า ระบบ ICAS มีมาตรการและกระบวนการจัดการความเสี่ยงด้านความน่าเชื่อถือด้านการปฏิบัติงาน (Operational reliability and availability) และการบริหารจัดการความต่อเนื่องทางธุรกิจส่วนใหญ่สอดคล้องกับมาตรฐานสากล PFMIIs โดยไม่พบประเด็นปัญหาที่ต้องแก้ไขอย่างเร่งด่วน

2.4.3 ระบบ ITMX (Interbank Transaction Management and Exchange)

สปท. กำกับดูแลระบบการโอนเงินรายย่อยระหว่างธนาคารของ NITMX ซึ่งจัดเป็นระบบการชำระเงินรายย่อยที่มีความสำคัญ โดยอาศัยอำนาจตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 (พ.ร.ฎ. e-Payment) รวมทั้งได้นำมาตรฐานสากล PFMIIs มาประยุกต์ใช้ในการกำกับดูแลระบบของ NITMX ด้วย โดยในปี 2558 สปท. ได้เข้าประเมินระบบตามมาตรฐานสากล PFMIIs ในลักษณะ onsite assessment สรุปผลประเมินได้ว่า ระบบของ NITMX มีการดำเนินการและการบริหารจัดการความเสี่ยงที่สำคัญส่วนใหญ่สอดคล้องกับมาตรฐาน PFMIIs เช่น ความเสี่ยงด้านกฎหมาย ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงการชำระดุล รวมทั้งมีการพัฒนาระบบให้บริการที่ตอบสนองต่อความต้องการของธนาคารสมาชิก เปิดเผยกฎระเบียบ วิธีปฏิบัติ หลักเกณฑ์ในการรับสมาชิก และข้อมูลที่ใช้เป็นการใช้บริการแก่สมาชิกและผู้เกี่ยวข้อง รวมทั้งมีกระบวนการในการสื่อสารรับส่งข้อมูลที่ได้มาตรฐาน โดยไม่พบประเด็นปัญหาที่ต้องปรับปรุงแก้ไขโดยทันทีหรือเร่งด่วน

2.5 มาตรฐานสากลที่เกี่ยวข้องในการดูแลระบบการชำระเงินที่สำคัญ

ในปี 2558 คณะทำงาน Cyber Resilience ภายใต้ CPMI-IOSCO : The Committee on Payments and Market Infrastructures (CPMI) และ The Technical Committee of the International Organization of Securities Commissions (IOSCO) ซึ่งเป็นคณะกรรมการที่กำหนดมาตรฐานสากล สำหรับการกำกับดูแลประสิทธิภาพและเสถียรภาพของระบบการชำระเงินและระบบที่เกี่ยวข้องด้านหลักทรัพย์ ภายใต้ Bank for International Settlements (BIS) ได้เผยแพร่ Consultative document เรื่อง “Guidance on cyber resilience for financial market infrastructures” เพื่อใช้เป็นแนวปฏิบัติเพิ่มเติม (supplementary) ของมาตรฐาน PFMI โดยสาระสำคัญสรุปได้ว่า ผู้ดำเนินการระบบโครงสร้างพื้นฐานในการทำธุรกรรมทางการเงิน (Financial Market Infrastructures : FMIs) และหน่วยงานกำกับดูแลควรสร้างความตระหนักถึงความเสี่ยงด้านไซเบอร์ ให้ทั่วถึงบุคลากรทุกระดับในองค์กร รวมทั้งคำนึงถึงความเชื่อมโยงกับระบบ FMIs ซึ่งอาจมีความเสี่ยงและผลกระทบที่เชื่อมโยงกันด้วย โดยให้มีการติดตามและวิเคราะห์ข้อมูลระบบเครือข่ายคอมพิวเตอร์อย่างเป็นระบบ เพื่อให้ใช้งานได้อย่างมีประสิทธิภาพ และมี



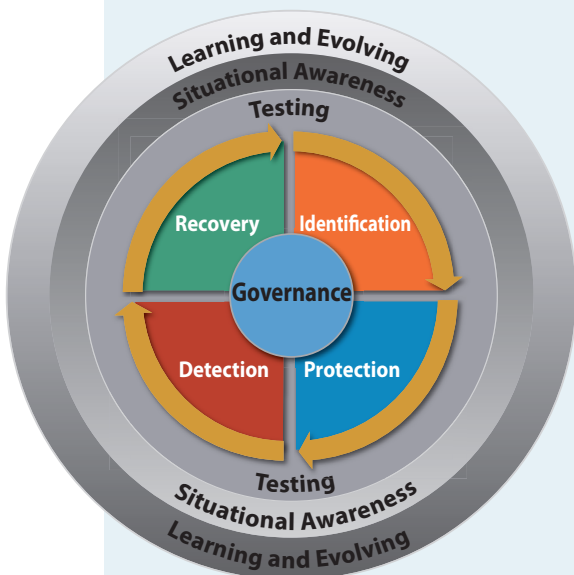
การทดสอบมาตรฐาน นอกจากนี่ยังให้ความสำคัญต่อการตอบสนองและกู้คืนให้ FMIs กลับมาทำงานต่อได้อย่างรวดเร็ว ซึ่ง BIS ได้เผยแพร่เอกสารฉบับสมบูรณ์แล้ว เมื่อเดือนมิถุนายน 2559 ทั้งนี้ ธปท. จะพิจารณานำแนวปฏิบัติมาประยุกต์ใช้ในการกำกับดูแลระบบการชำระเงินที่สำคัญต่อไป

กรอบที่ 7: Cyber Resilience for Financial Market Infrastructure

Cyber resilience คือ ความสามารถในการเตรียมการ ด้านทาน ควบคุมสถานการณ์ และฟื้นฟูระบบให้คืนสู่สภาวะปกติโดยเร็ว หลังจากถูกโจมตีทางไซเบอร์

การเสริมสร้าง cyber resilience ของระบบการชำระเงินที่มีความสำคัญที่จัดเป็นโครงสร้างพื้นฐานการทำธุรกรรมทางการเงิน (FMI) นั้น ถือเป็นสิ่งสำคัญที่ช่วยส่งเสริมให้ระบบการชำระเงินมีประสิทธิภาพและดำเนินการได้โดยสอดคล้องตามหลักการของมาตรฐานสากล PFMI สามารถทำธุรกรรมทางการเงินได้อย่างต่อเนื่อง โดยมีการบริหารจัดการความเสี่ยงด้านปฏิบัติการที่เหมาะสมและมีกระบวนการกู้คืนระบบได้รวดเร็วภายใน 2 ชั่วโมงหลังจากเกิดเหตุหยุดชะงักจากภัยคุกคามด้านไซเบอร์ และสามารถจัดการให้การชำระเงินเสร็จสมบูรณ์ได้ภายในวันที่เกิดเหตุ

เพื่อให้ระบบ FMI มีกรอบแนวทางดำเนินงานในการเสริมสร้าง cyber resilience CPMI-IOSCO ได้จัดทำ Guidance on cyber resilience for financial market infrastructures เพื่อเป็นแนวทางให้ระบบ FMI นำไปประยุกต์ใช้ โดยองค์ประกอบสำคัญของการสร้าง cyber resilience มี 5 องค์ประกอบหลัก (GIPDR) ได้แก่



Governance: การจัดทำมีมาตรการ กระบวนการและทรัพยากรที่จำเป็นสำหรับการบริหารจัดการความเสี่ยงด้านไซเบอร์

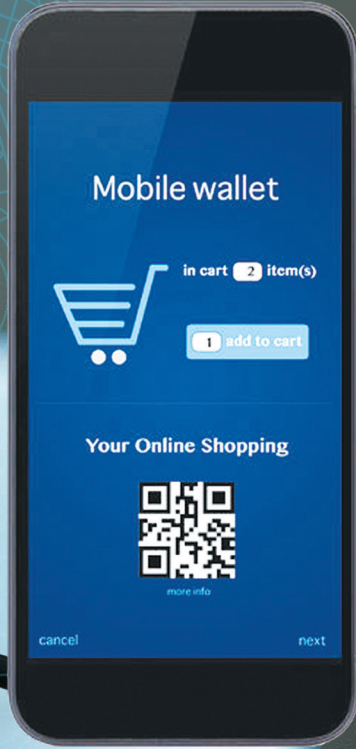
Identification: การระบุสิ่งที่มีผลต่อการปฏิบัติงานสำคัญ ไม่ว่าจะเป็นกระบวนการ ระบบงาน หรือระบบที่เชื่อมโยง

Protection: การกำหนดมาตรการควบคุมและออกแบบกระบวนการเพื่อปกป้องสิ่งสำคัญดังกล่าว

Detection: การติดตามตรวจจับเหตุคุกคามทางไซเบอร์ได้อย่างรวดเร็วทันการณ์

Recovery: การควบคุมสถานการณ์และลดความเสียหาย โดยต้องสามารถฟื้นฟูระบบอย่างรวดเร็วและปลอดภัยให้ FMI สามารถดำเนินการต่อไปได้

นอกจากนี้ ยังมีการดำเนินการที่สำคัญอีก 3 ด้าน ที่จำเป็นในการสร้าง cyber resilience ได้แก่ การทดสอบว่ามาตรการที่กำหนดไว้สามารถบรรลุเป้าหมายที่ต้องการหรือไม่ (Testing) การตระหนักรู้ในสถานการณ์ภัยคุกคามเพื่อจะได้เตรียมการรับมือให้เหมาะสม (Situational Awareness) และการเรียนรู้เพื่อประเมินและปรับปรุงให้มีความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ใหม่ ๆ ได้อย่างต่อเนื่อง (Learning and Evolving)



3

การกำกับดูแลผู้ให้บริการ การชำระเงินทางอิเล็กทรอนิกส์

3.1 การปรับปรุงกฎหมายและประกาศหลักเกณฑ์ที่เกี่ยวข้อง ในการกำกับดูแลผู้ให้บริการ

ในปี 2558 ธปท. ได้พิจารณาทบทวนปรับปรุงกฎหมายและหลักเกณฑ์ต่าง ๆ ที่เกี่ยวข้อง ดังนี้

- 1) ปรับปรุงหลักเกณฑ์ วิธีการ และเงื่อนไขการกำกับดูแลภายใต้พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 ซึ่งเป็นกฎหมายลำดับรองภายใต้พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ประกอบด้วย การปรับปรุงประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) และประกาศ ธปท. เพื่อให้มีความเหมาะสมและสอดคล้องกับสภาวะแวดล้อมทางเศรษฐกิจและรูปแบบการดำเนินธุรกิจที่เปลี่ยนแปลงไป ซึ่งประกาศ คธอ. และประกาศ ธปท. ได้ลงประกาศในราชกิจจานุเบกษาแล้ว สรุปสาระสำคัญในการปรับปรุงได้ดังนี้
 - ปรับปรุงหลักเกณฑ์เรื่องการกำกับดูแลสถานภาพทางการเงินของผู้ให้บริการให้มีความมั่นคงสามารถดำเนินธุรกิจและให้บริการได้อย่างต่อเนื่อง
 - กำหนดคุณสมบัติและลักษณะต้องห้ามของกรรมการหรือผู้ซึ่งมีอำนาจจัดการเพิ่มเติม
 - ขยายขอบเขตการประกอบธุรกิจของผู้ให้บริการเงินอิเล็กทรอนิกส์ (e-Money) เช่น ให้ออก e-Money เป็นสกุลเงินตราต่างประเทศหรือใช้ในต่างประเทศได้ ให้ประกอบธุรกิจอื่นที่สนับสนุนธุรกิจ e-Payment โดยผู้ให้บริการจะต้องขออนุญาตจาก ธปท. ก่อน นอกจากนี้ ยังกำหนดให้ผู้ให้บริการดำรงอัตราส่วนของผู้ถือหุ้นสุทธิต่อยอดคงค้างของเงินที่ได้รับล่วงหน้า ณ สิ้นไตรมาส ไม่ต่ำกว่าที่กำหนด เพื่อดูแลความเสี่ยงต่อฐานะและความมั่นคงทางการเงิน
- 2) ปรับปรุงหลักเกณฑ์ วิธีการ และเงื่อนไขการกำกับดูแลภายใต้ประกาศกระทรวงการคลัง เรื่อง กิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (การประกอบธุรกิจบัตรเงินอิเล็กทรอนิกส์) เพื่อให้มีความเหมาะสมและสอดคล้องกับการเปลี่ยนแปลงของสภาพแวดล้อมทางธุรกิจ มีการกำกับดูแลความเสี่ยงของผู้ให้บริการที่มีประสิทธิภาพขึ้น และสอดคล้องกับหลักเกณฑ์ของประกาศ คธอ. เช่น การกำหนดคุณสมบัติและลักษณะต้องห้ามของกรรมการหรือผู้ซึ่งมีอำนาจจัดการ การขยายขอบเขตการให้บริการ การรายงานการเปิด/ย้าย/ปิด สำนักงานสาขา ซึ่งประกาศกระทรวงการคลังและประกาศ ธปท. ได้ลงประกาศในราชกิจจานุเบกษาแล้ว

- 3) ยกร่างพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ของสถาบันการเงิน เฉพาะกิจ พ.ศ. 2559 ภายใต้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เพื่อกำกับดูแล การให้บริการการชำระเงินทางอิเล็กทรอนิกส์ของสถาบันการเงินเฉพาะกิจให้มีมาตรฐานเดียวกันกับผู้ให้บริการ การชำระเงินทางอิเล็กทรอนิกส์ที่เป็นสถาบันการเงินและที่มีใช้สถาบันการเงินตามที่ได้รับมอบหมายจาก คธอ. ซึ่งได้รับความเห็นชอบจากคณะรัฐมนตรี และประกาศลงราชกิจจานุเบกษาแล้ว และจะมีผลใช้บังคับตั้งแต่วันที่ 28 กรกฎาคม 2559 ขณะนี้ ธปท. อยู่ระหว่างจัดทำประกาศหลักเกณฑ์ เพื่อกำกับดูแลการให้บริการการชำระเงิน ทางอิเล็กทรอนิกส์ของสถาบันการเงินเฉพาะกิจภายใต้พระราชกฤษฎีกาดังกล่าวต่อไป

3.2 การกำกับและตรวจสอบผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์

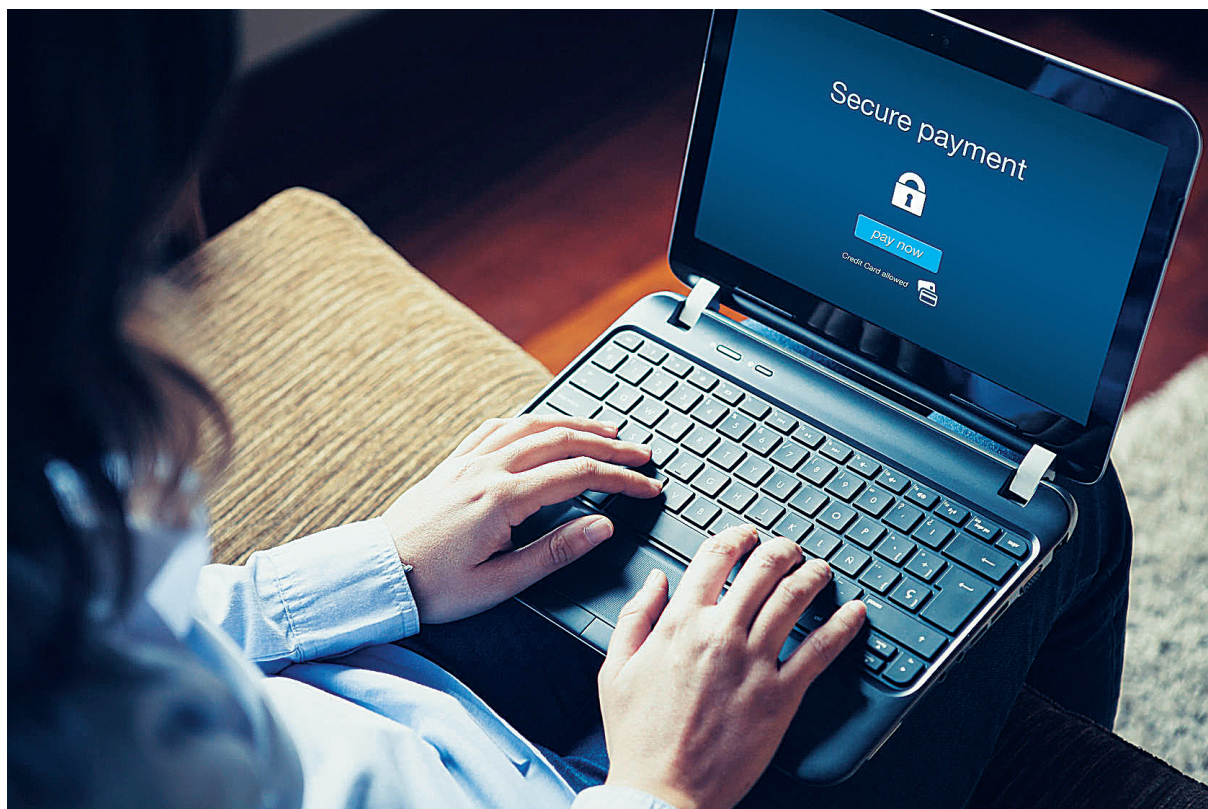
ธปท. กำกับดูแลและตรวจสอบผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์เพื่อให้มีการบริหารความเสี่ยงที่เหมาะสมในการให้บริการธุรกรรมทางการเงิน รวมทั้งให้มีความน่าเชื่อถือและมีความปลอดภัยในการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ ตลอดจนเพิ่มศักยภาพในการแข่งขันของภาคธุรกิจและการให้บริการของภาครัฐ โดย ธปท. เป็นผู้ควบคุมดูแลผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ที่สำคัญตามกฎหมายที่เกี่ยวข้อง ได้แก่ ผู้ประกอบธุรกิจบัตร เงินอิเล็กทรอนิกส์ (e-Money) ตามประกาศของคณะปฏิวัติ ฉบับที่ 58 และผู้ประกอบธุรกิจบริการการชำระเงินทาง อิเล็กทรอนิกส์ตามพระราชกฤษฎีกาว่าด้วยการควบคุม ดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551

3.2.1 การกำกับดูแลตามประกาศกระทรวงการคลัง เรื่อง กิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (การประกอบธุรกิจบัตรเงินอิเล็กทรอนิกส์)

ธปท. กำกับดูแลผู้ประกอบธุรกิจบัตรเงินอิเล็กทรอนิกส์ที่มีใช้สถาบันการเงิน ซึ่งได้รับอนุญาตตามประกาศกระทรวงการคลัง เรื่อง กิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (การประกอบธุรกิจบัตรเงินอิเล็กทรอนิกส์) (ปว. 58) ลงวันที่ 4 ตุลาคม 2547

ในปี 2558 มีผู้ขอรับใบอนุญาตประกอบธุรกิจ e-Money จำนวน 4 ราย เป็นการประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ผ่านแอปพลิเคชันบนโทรศัพท์เคลื่อนที่ เพื่อใช้ชำระค่าสินค้าและบริการ ณ ร้านค้าที่ร่วมให้บริการ และชำระค่าสินค้าและบริการผ่านช่องทางออนไลน์ โดย ณ สิ้นปี 2558 มีจำนวนผู้ให้บริการ e-Money ภายใต้ ปว. 58 ทั้งสิ้น 12 ราย





3.2.2 การควบคุมดูแลตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 (พ.ร.ฎ. e-Payment)

รพท. มีหน้าที่ควบคุมดูแลผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ โดยอาศัยอำนาจตาม พ.ร.ฎ. e-Payment ซึ่งเป็นกฎหมายที่อยู่ภายใต้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 โดยมีระดับการควบคุมดูแล 3 ระดับ คือ บัญชี ก เป็นธุรกิจบริการที่ต้องแจ้งให้ทราบ บัญชี ข เป็นธุรกิจบริการที่ต้องขอขึ้นทะเบียน และบัญชี ค เป็นธุรกิจบริการที่ต้องได้รับใบอนุญาตก่อนให้บริการ ในปี 2558 รพท. ได้ดำเนินการควบคุมดูแลผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ตาม พ.ร.ฎ. e-Payment สรุปได้ ดังนี้

- 1) พิจารณาการแจ้งให้ทราบก่อนให้บริการของผู้ที่ประสงค์จะเป็นผู้ให้บริการตามบัญชี ก พิจารณาการขอขึ้นทะเบียนของผู้ที่ประสงค์จะเป็นผู้ให้บริการตามบัญชี ข และพิจารณาการขอรับใบอนุญาตของผู้ที่ประสงค์จะเป็นผู้ให้บริการตามบัญชี ค เสนอ คธอ. เพื่อพิจารณาออกใบอนุญาต โดยในปี 2558 มีผู้แจ้งเพื่อทราบ 1 ราย ขอขึ้นทะเบียน 1 ราย และขอใบอนุญาต 13 ราย ในจำนวนนี้ ส่วนใหญ่เป็นผู้ให้บริการรับชำระค่าสินค้าและบริการทางอินเทอร์เน็ต (payment gateway) บริการเงินอิเล็กทรอนิกส์ (e-Money) และบริการรับชำระเงินแทน นอกจากนี้ มีผู้ให้บริการที่คืนใบขึ้นทะเบียนตามบัญชี ข จำนวน 1 ราย และคืนใบอนุญาตตามบัญชี ค จำนวน 3 ราย

ณ สิ้นปี 2558 มีผู้ให้บริการที่แจ้งให้ทราบตามบัญชี ก จำนวน 1 ราย ผู้ให้บริการที่ได้รับการขึ้นทะเบียนตามบัญชี ข จำนวน 9 ราย และผู้ให้บริการที่ได้รับใบอนุญาตตามบัญชี ค จำนวน 93 ราย⁷ (ธนาคารพาณิชย์ 31 ราย และผู้ให้บริการที่มีใช้สถาบันการเงิน 62 ราย) รวมใบอนุญาตทั้งสิ้น 145 ฉบับ

ภาพที่ 8 : ภาพรวมธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

บัญชี ก	Non-bank 1 ราย			บัญชี ข	Bank	ไม่มี	บัญชี ค	Bank	31 ราย	
	Bank	Non-Bank	รวม		Non-bank	9 ราย		Non-bank	62 ราย	
ก e-Money	-	1	1	ข (1) เครือข่ายบัตรเครดิต	-	-	ค (1) Clearing	-	3	3
รวมใบรับแจ้ง (ฉบับ)	-	1	1	ข (2) เครือข่าย EDC	-	-	ค (2) Settlement	3	-	3
จำนวน (ราย)	-	1	1	ข (3) Switching	-	4	ค (3) e-Payment	31	45	76
				ข (4) e-Money	-	5	ค (4) Switching	-	3	3
				รวมใบขึ้นทะเบียน (ฉบับ)	-	9	ค (5) Bill Payment	19	21	40
				จำนวน (ราย)	-	9	ค (6) e-Money	8	12	20
							รวมใบอนุญาต (ฉบับ)	61	84	145
							จำนวน (ราย)	31	62	93

ที่มา: ธนาคารแห่งประเทศไทย

ข้อมูล ณ วันที่ 30 ธันวาคม 2558

- กำกับดูแลและตรวจสอบผู้ให้บริการ (Off-site examination) ให้ปฏิบัติตาม พ.ร.ฎ. e-Payment และประกาศต่าง ๆ ที่เกี่ยวข้อง การติดตามเรื่องร้องเรียนเกี่ยวกับผู้ประกอบการ ติดตามตรวจสอบข้อเท็จจริงเพื่อกำกับดูแล ให้ปฏิบัติตามกฎหมาย โดยในปี 2558 มีการรายงานกรณีปฏิบัติไม่เป็นไปตามหลักเกณฑ์ที่กฎหมายกำหนด โดยเป็นประเด็นที่ไม่มีผลกระทบต่อการใช้บริการ ซึ่งได้รายงานผลการควบคุมดูแลและการไม่ปฏิบัติตามกฎหมายของผู้ให้บริการต่อ คธอ. และแจ้งผู้ให้บริการรับทราบและดำเนินการแล้ว

⁷ สามารถดูรายชื่อผู้ประกอบการธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ได้จากเว็บไซต์ของ ธปท. (<http://www.bot.or.th/> ระบบการชำระเงิน/การกำกับดูแล e-Payment/รายชื่อผู้ประกอบการ)



- 3) ตรวจสอบผู้ให้บริการ e-Payment ณ สำนักงานของผู้ให้บริการ (On-site examination) โดยในปี 2558 ธปท. ได้เข้าตรวจสอบและสังเกตการณ์การปฏิบัติงานของผู้ให้บริการ e-Payment ที่มีใช้สถาบันการเงิน ซึ่งเป็นผู้ให้บริการในกลุ่มบัญชี ค โดยพิจารณาจากประเภทธุรกิจบริการที่มีผู้ใช้บริการแพร่หลาย มีผลกระทบต่อผู้ใช้บริการในวงกว้าง ฐานะความมั่นคงของผู้ให้บริการ รวมถึงข้อร้องเรียนที่ได้รับจากผู้ใช้บริการ ซึ่ง ธปท. ได้ตรวจสอบและประเมินการดำเนินการของผู้ให้บริการทั้งในด้านการบริหารจัดการการให้บริการ e-Payment และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และได้แจ้งประเด็นที่ตรวจพบให้แก่ผู้ให้บริการทราบและปรับปรุงให้มีการดำเนินการที่ครอบคลุมและรัดกุมเพียงพอ สามารถให้บริการได้อย่างต่อเนื่อง มีประสิทธิภาพ มีการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศตามมาตรฐาน มีการให้บริการอย่างเป็นธรรมต่อผู้บริโภคหรือผู้ใช้บริการ และมีการปฏิบัติที่เป็นไปตามหลักเกณฑ์ที่กฎหมายกำหนด เพื่อสร้างความมั่นใจในการใช้บริการการชำระเงินทางอิเล็กทรอนิกส์