ใช้สำหรับการประชุมชี้แจง
ในวันที่ 27 กุมภาพันธ์ 2561

ประกาศธนาคารแห่งประเทศไทย
ที่ สนช. /2561
เรื่อง หลักเกณฑ์การกำกับดูแลผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ

---

1. เหตุผลในการออกประกาศ

ระบบการชำระเงินที่มีความสำคัญเป็นระบบโครงสร้างพื้นฐานหลักของประเทศ โดยเป็นระบบการชำระเงินที่รองรับการโอนเงินมูลค่าสูง หรือที่ใช้สำหรับการหักบัญชีหรือการชำระดุลที่เชื่อมโยงระหว่างธนาคารกลางกับผู้ประกอบธุรกิจระบบการชำระเงินต่าง ๆ ซึ่งเป็นสมาชิกของระบบการชำระเงินที่มีความสำคัญ รวมถึงมีความเชื่อมโยง (interdependencies) กับระบบการซื้อขายหลักทรัพย์ในตลาดหลักทรัพย์และระบบอื่น ๆ ที่เกี่ยวข้อง เพื่อสนับสนุนการทำธุรกรรมทางการเงินให้สามารถดำเนินการได้อย่างสะดวก รวดเร็ว และมีประสิทธิภาพ ช่วยส่งเสริมการขับเคลื่อนกิจกรรมทางเศรษฐกิจและรักษาเสถียรภาพทางการเงินของประเทศ (financial stability) ซึ่งหากระบบหยุดชะงักอาจส่งผลกระทบต่อประโยชน์สาธารณะ ความเชื่อมั่นของสาธารณชน หรือเสถียรภาพและความมั่นคงของระบบการชำระเงิน

ธนาคารแห่งประเทศไทยจึงกำหนดหลักเกณฑ์การกำกับดูแลระบบการชำระเงินที่มีความสำคัญ โดยนำหลักการตามมาตรฐานสากลมาใช้ มีการกำหนดหลักเกณฑ์เกี่ยวกับการคุ้มครองผลสิ้นสุดของการชำระเงิน (payment finality) และการรองรับกรณีที่สมาชิกถูกศาลสั่งพิทักษ์ทรัพย์หรือล้มละลาย รวมถึงกำกับดูแลในด้านการบริหารจัดการตามหลักธรรมาภิบาล ด้านการบริหารความเสี่ยงและความปลอดภัย ด้านการคุ้มครองสมาชิกและสาธารณชน และด้านการส่งเสริมประสิทธิภาพ เพื่อส่งเสริมให้ระบบการชำระเงินที่มีความสำคัญมีประสิทธิภาพ มั่นคง ปลอดภัย และบริหารจัดการความเสี่ยงได้อย่างเหมาะสม รวมถึงสามารถให้บริการได้อย่างต่อเนื่องทั้งในภาวะปกติและภาวะฉุกเฉิน รวมถึงลดความเสี่ยงที่อาจก่อให้เกิดผลกระทบต่อเนื่องเป็นวงกว้าง (systemic risk) ซึ่งนำไปสู่การมีเสถียรภาพของระบบชำระเงินและระบบการเงินโดยรวม

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 7 แห่งพระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560 ธนาคารแห่งประเทศไทยกำหนดหลักเกณฑ์การกำกับดูแลผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ

3. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ตามกฎหมายว่าด้วยระบบการชำระเงิน

4. เนื้อหา

4.1 นิยาม

ในประกาศฉบับนี้

“ระบบการชำระเงินที่มีความสำคัญ” หมายความว่า ระบบการชำระเงินที่มีความสำคัญต่อความมั่นคงหรือเสถียรภาพของระบบการชำระเงิน ระบบสถาบันการเงิน หรือระบบการเงินของประเทศ

“ผู้ให้บริการ” หมายความว่า ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ

“สมาชิก” หมายความว่า ผู้ใช้บริการที่ยินยอมผูกพันตามหลักเกณฑ์ในการใช้บริการระบบการชำระเงินที่มีความสำคัญ

“ธปท.” หมายความว่า ธนาคารแห่งประเทศไทยตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย

“คณะกรรมการ” หมายความว่า คณะกรรมการระบบการชำระเงินตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย หรือคณะกรรมการของผู้ให้บริการระบบการชำระเงินที่มีความสำคัญตามที่รัฐมนตรีประกาศกำหนด

4.2 หลักเกณฑ์การกำกับดูแล

ผู้ให้บริการต้องปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไข ดังต่อไปนี้

4.2.1 การคุ้มครองผลสมบูรณ์ของการชำระเงิน (payment finality)

ให้รายการโอนเงินหรือชำระดุลที่สมาชิกส่งเข้าระบบการชำระเงินที่มีความสำคัญมีผลสมบูรณ์ เมื่อมีการบันทึกผลการโอนเงินหรือชำระดุลในระบบตามหลักเกณฑ์ของระบบที่ผู้ให้บริการกำหนด โดยผู้ให้บริการ สมาชิก หรือผู้ที่เกี่ยวข้องจะเพิกถอน กลับรายการ แก้ไข หยุด หรือระงับรายการมิได้

ทั้งนี้ ผู้ให้บริการต้องกำหนดหลักเกณฑ์ เงื่อนไข และขั้นตอนการดำเนินการที่เกี่ยวข้องกับการโอนเงินหรือการชำระดุลเกี่ยวกับผลสมบูรณ์ของการโอนเงินหรือการชำระดุล โดยกำหนดกระบวนการ ระยะเวลาในการชำระเงิน และจุดที่การโอนเงินหรือการชำระดุลมีผลสมบูรณ์ (point of finality) ตลอดจนมีแนวปฏิบัติเพื่อรองรับหลักเกณฑ์ดังกล่าวอย่างชัดเจน

4.2.2 การดำเนินการรองรับกรณีที่สมาชิกถูกศาลสั่งพิทักษ์ทรัพย์หรือล้มละลาย

(1) กำหนดกระบวนการและพิธีปฏิบัติ รวมถึงแนวทางการประสานงานระหว่างผู้เกี่ยวข้อง รองรับกรณีที่สมาชิกถูกศาลสั่งพิทักษ์ทรัพย์หรือล้มละลาย เพื่อให้สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที ลดความเสี่ยงที่จะเกิดความเสียหายและปัญหาด้านสภาพคล่องที่อาจเกิดขึ้น

(2) จัดให้มีการทดสอบร่วมกับสมาชิกและผู้ที่เกี่ยวข้อง รวมถึงทบทวนกระบวนการและพิธีปฏิบัติรองรับกรณีสมาชิกถูกศาลสั่งพิทักษ์ทรัพย์หรือล้มละลายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับกระบวนการและพิธีปฏิบัติที่ได้กำหนดไว้

4.2.3 ด้านการบริหารจัดการตามหลักธรรมาภิบาล

(1) การควบคุมภายใน

(1.1) จัดให้มีโครงสร้างองค์กร โดยกำหนดหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องในการกำกับดูแล ควบคุม และตรวจสอบการดำเนินงานที่เหมาะสม รวมถึงมีสายการบังคับบัญชาและการรายงานที่ชัดเจน เพื่อให้มีการสอบทานและถ่วงดุลอำนาจอย่างเหมาะสม

(1.2) จัดให้มีกระบวนการควบคุมภายใน ซึ่งครอบคลุมถึงการตรวจสอบรายการผิดปกติ เพื่อป้องกันความเสี่ยงจากความผิดพลาดหรือการทุจริตในการปฏิบัติงาน หรือการบริหารความเสี่ยงที่ไม่เหมาะสมและรัดกุมเพียงพอ หรือการไม่ปฏิบัติตามกฎ ระเบียบ หรือข้อบังคับภายในของผู้ให้บริการ หรือกฎหมายที่เกี่ยวข้อง

(2) การรายงานการดำเนินงานและแผนงานที่สำคัญ

ให้รายงานการดำเนินงานและแผนงานที่สำคัญที่เกี่ยวข้องกับระบบการชำระเงินที่มีความสำคัญแก่คณะกรรมการโดยสม่ำเสมอ เพื่อติดตามการดำเนินงาน เช่น การนำเสนอเป้าหมายในการให้บริการ การรายงานระดับความพร้อมใช้งานของระบบ (system availability) และแผนการปรับเปลี่ยนระบบงานที่สำคัญ

4.2.4 ด้านการบริหารความเสี่ยงและความปลอดภัย

ผู้ให้บริการต้องปฏิบัติตามประกาศ ธปท. ว่าด้วยนโยบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ (IT Security) และต้องปฏิบัติเพิ่มเติมตามหลักเกณฑ์ดังต่อไปนี้

(1) นโยบายและมาตรการบริหารความเสี่ยง

กำหนดนโยบายและมาตรการบริหารความเสี่ยงในด้านต่าง ๆ ที่เกี่ยวข้องกับระบบ เช่น ความเสี่ยงด้านเครดิต ความเสี่ยงด้านสภาพคล่อง และความเสี่ยงด้านปฏิบัติการ ซึ่งรวมถึงการระบุระดับความเสี่ยงที่ยอมรับได้ (risk appetite) ทั้งที่เกิดจากระบบของผู้ให้บริการ สมาชิก และระบบที่มีความเชื่อมโยงกัน (interdependencies)

ทั้งนี้ นโยบายและมาตรการบริหารความเสี่ยงดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการ และต้องจัดให้มีการทบทวนนโยบายและมาตรการบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้ง

(2) นโยบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

ต้องจัดให้มีการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศโดยผู้ตรวจสอบภายนอกอย่างน้อยปีละ 1 ครั้ง ซึ่งขอบเขตในการตรวจสอบต้องรวมถึงการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) และจัดให้มีการทดสอบเจาะระบบ (Penetration Test) เพื่อทดสอบประสิทธิภาพของเทคโนโลยีการรักษาความมั่นคงปลอดภัย

ทั้งนี้ ในการตรวจสอบระบบสารสนเทศ ผู้ให้บริการต้องเลือกใช้ผู้ตรวจสอบภายนอกที่เป็นอิสระ มีความรู้ความสามารถในการตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศได้

ในกรณีมีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ทำให้ผู้ให้บริการไม่สามารถดำเนินการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศตามหลักเกณฑ์และระยะเวลาที่กำหนดได้ ให้ผู้ให้บริการยื่นขออนุญาตผ่อนผันเพื่อขยายระยะเวลาต่อ ธปท. พร้อมชี้แจงเหตุผลความจำเป็น และกำหนดเวลาที่จะดำเนินการแล้วเสร็จ โดย ธปท. อาจพิจารณาขยายระยะเวลาหรือไม่ก็ได้

(3) การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP)

(3.1) กำหนดนโยบายการบริหารความต่อเนื่องทางธุรกิจ โดยมีการวิเคราะห์และประเมินผลกระทบต่อการหยุดชะงักของระบบที่ให้บริการ รวมทั้งจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

(3.2) จัดให้มีการทบทวนและทดสอบการปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องร่วมกับสมาชิกและผู้ที่เกี่ยวข้องอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(4) การใช้บริการจากผู้ให้บริการภายนอก

หากมีการใช้บริการจากผู้ให้บริการภายนอก เพื่อดำเนินการแทนในงานระบบสารสนเทศและงานอื่นใดที่มีผลกระทบต่อการให้บริการระบบอย่างมีนัยสำคัญ (critical service provider) ผู้ให้บริการต้องดำเนินการในเรื่องดังต่อไปนี้

(4.1) กำหนดนโยบายการใช้บริการจากผู้ให้บริการภายนอก โดยครอบคลุมถึงการบริหารความเสี่ยงที่เกิดจากการใช้บริการจากผู้ให้บริการภายนอก การรักษาความปลอดภัยและความลับของระบบและข้อมูล การรักษาความถูกต้องเชื่อถือได้ของระบบและข้อมูล และการรักษาความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ

(4.2) จัดให้มีการประเมินและการบริหารความเสี่ยงที่อาจเกิดขึ้นให้ครอบคลุมถึงการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล และความเสี่ยงอันเนื่องมาจากการใช้บริการจากผู้ให้บริการภายนอก (interdependency risk) จนอาจทำให้การเปลี่ยนแปลงหรือยกเลิกการใช้บริการทำได้ยาก (vendor lock-in) รวมถึงความเสี่ยงจากการกระจุกตัวของทรัพยากรที่สำคัญ (concentration risk) โดยเฉพาะกรณีที่ผู้ให้บริการภายนอกมีการให้บริการแก่ผู้ใช้บริการหลายราย

(4.3) จัดให้มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ที่ครอบคลุมถึงการใช้บริการจากผู้ให้บริการภายนอก เพื่อรองรับกรณีการเกิดปัญหาหรือเหตุการณ์ผิดปกติจากการใช้บริการจากผู้ให้บริการภายนอกและเพื่อลดผลกระทบที่อาจเกิดขึ้น

4.2.5 ด้านการคุ้มครองสมาชิกและสาธารณชน

(1) การเข้าร่วมและการออกจากระบบ (access and exit regime)

(1.1) กำหนดวัตถุประสงค์ หลักเกณฑ์ เงื่อนไข วิธีปฏิบัติ และค่าธรรมเนียมหรือค่าใช้จ่ายที่เกี่ยวข้องในการเข้าร่วมและการออกจากระบบของสมาชิกไว้อย่างชัดเจนเป็นลายลักษณ์อักษร โดยคำนึงถึงหลักการในการเข้าถึงบริการที่เป็นธรรมและเปิดกว้าง (fair and open access) ซึ่งไม่มีการผูกขาดหรือกีดกันการแข่งขัน และเปิดเผยให้สมาชิกและสาธารณชนทราบโดยทั่วถึง

(1.2) จัดให้มีการประเมินความเสี่ยงและวิเคราะห์ผลกระทบที่เกี่ยวข้องจากการรับสมาชิกรายใหม่ที่เข้าร่วมใช้ระบบ เช่น ฐานะทางการเงิน ความพร้อมในการเชื่อมต่อและใช้ระบบ เพื่อให้มั่นใจว่าการรับสมาชิกรายใหม่จะไม่ก่อให้เกิดความเสี่ยงและผลกระทบต่อการใช้บริการของสมาชิกรายเดิม

(1.3) เปิดเผยรายชื่อสมาชิกที่เป็นปัจจุบัน ให้สมาชิกและสาธารณชนทราบโดยทั่วถึง

(2) การกำหนดและเปิดเผยข้อตกลงการให้บริการ

กำหนดข้อตกลงในการให้บริการไว้เป็นลายลักษณ์อักษร และ เปิดเผยให้สมาชิกทราบอย่างชัดเจนและเป็นปัจจุบัน ซึ่งอย่างน้อยต้องประกอบด้วย

(2.1) สิทธิ หน้าที่ และความรับผิดของผู้ให้บริการและสมาชิก ทั้งในกรณีปกติและกรณีที่เกิดเหตุฉุกเฉิน

(2.2) หลักเกณฑ์ เงื่อนไข และวิธีปฏิบัติในการให้บริการ

(2.3) ความเสี่ยงทางการเงิน (financial risk) หรือความเสี่ยงอื่นใดที่อาจเกิดขึ้นจากการใช้บริการ (ถ้ามี) เพื่อให้สมาชิกสามารถประเมินความเสี่ยงที่เกี่ยวข้องจากการใช้บริการได้

ทั้งนี้ ผู้ให้บริการมีหน้าที่ติดตามดูแลให้สมาชิกปฏิบัติตามหลักเกณฑ์เงื่อนไขที่กำหนด โดยจัดให้มีวิธีการดำเนินการกับสมาชิกที่ฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์และเงื่อนไขที่กำหนด และในกรณีที่ผู้ให้บริการมีการเปลี่ยนแปลงหลักเกณฑ์ดังกล่าว ซึ่งทำให้สมาชิกเสียประโยชน์ ผู้ให้บริการต้องแจ้งให้สมาชิกทราบล่วงหน้า โดยแจ้งข้อมูลผ่านช่องทางอิเล็กทรอนิกส์ หรือแจ้งเป็นลายลักษณ์อักษร หรือด้วยวิธีการอื่นใดให้สมาชิกสามารถทราบได้

(3) การแจ้งข้อมูลให้สมาชิกรายอื่นทราบกรณีมีการระงับการให้บริการหรือการเพิกถอนการให้บริการกับสมาชิกรายใดรายหนึ่ง

(3.1) กรณีการระงับเป็นการชั่วคราวหรือเพิกถอนการให้บริการกับสมาชิกรายใดรายหนึ่ง ผู้ให้บริการต้องแจ้งให้สมาชิกรายอื่นทราบโดยทันที

(3.2) กรณีสมาชิกขอลาออกจากระบบ ผู้ให้บริการต้องแจ้งให้สมาชิกรายอื่นทราบล่วงหน้า 15 วัน ผ่านช่องทางอิเล็กทรอนิกส์ หรือแจ้งเป็นลายลักษณ์อักษร หรือด้วยวิธีการอื่นใดเพื่อให้สมาชิกสามารถทราบได้

(4) การเก็บรักษาข้อมูลส่วนบุคคลของสมาชิก

(4.1) กำหนดนโยบายในการเก็บรักษาข้อมูลของสมาชิก การกำหนดชั้นความลับในการเข้าถึงข้อมูล และการระบุตัวบุคคลที่มีสิทธิเข้าถึงข้อมูลดังกล่าว พร้อมทั้งจัดให้มีระบบการจัดเก็บข้อมูลที่ถูกต้องเชื่อถือได้ และป้องกันผู้ที่ไม่มีหน้าที่เกี่ยวข้องเข้าถึงหรือแก้ไขข้อมูลที่เก็บรักษา

(4.2) รักษาความลับข้อมูลส่วนบุคคลของสมาชิก โดยจะไม่เปิดเผยข้อมูลเหล่านั้นตลอดระยะเวลาการใช้บริการและภายหลังที่เลิกใช้บริการแล้วเว้นแต่กรณีต่อไปนี้

(4.2.1) การเปิดเผยโดยได้รับความยินยอมจากสมาชิกเป็นหนังสือหรือด้วยวิธีการอื่นใดทางอิเล็กทรอนิกส์ตามที่ผู้ให้บริการกำหนด

(4.2.2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(4.2.3) การเปิดเผยแก่ผู้สอบบัญชีของผู้ให้บริการ

(4.2.4) การเปิดเผยเพื่อประโยชน์ในการกำหนดนโยบายและกำกับดูแลระบบการชำระเงินของ ธปท.

(4.2.5) การเปิดเผยเพื่อประโยชน์ในการปฏิบัติตามกฎหมาย

(5) การเปิดเผยค่าธรรมเนียม

(5.1) เปิดเผยรายละเอียดของค่าธรรมเนียมที่เรียกเก็บจากสมาชิก ซึ่งรวมถึงนโยบายการให้ส่วนลด (discount policies) (ถ้ามี) ให้สมาชิกและสาธารณชนทราบโดยทั่วถึง

ทั้งนี้ ในการกำหนดค่าธรรมเนียม ผู้ให้บริการต้องคำนึงถึงความเป็นธรรมต่อสมาชิกด้วย

(5.2) กรณีที่มีการเปลี่ยนแปลงค่าธรรมเนียม ผู้ให้บริการจะต้องแจ้งให้สมาชิกทราบล่วงหน้าไม่น้อยกว่า 30 วันก่อนการเปลี่ยนแปลงจะมีผลใช้บังคับ โดยแจ้งข้อมูลรายละเอียดการเปลี่ยนแปลงผ่านช่องทางอิเล็กทรอนิกส์ หรือแจ้งเป็นลายลักษณ์อักษร หรือด้วยวิธีการอื่นใดเพื่อให้สมาชิกสามารถทราบได้

4.2.6 ด้านการส่งเสริมประสิทธิภาพ

(1) การให้บริการอย่างมีประสิทธิภาพ

(1.1) จัดให้มีการสำรวจและรับฟังความคิดเห็นของสมาชิกในเรื่องเกี่ยวกับการให้บริการที่สำคัญอย่างสม่ำเสมอ เช่น ขอบเขตในการให้บริการ ฟังก์ชั่นในการใช้งานระบบหรือทางเลือกในการใช้เทคโนโลยีหรือกระบวนการ เป็นต้น เพื่อพัฒนาและปรับปรุงให้ระบบตอบสนองความต้องการของสมาชิก และทันต่อความเปลี่ยนแปลงของเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็ว

(1.2) กำหนดเป้าหมายในการให้บริการที่สามารถประเมินและวัดผลได้ เช่น ระดับความพร้อมใช้งานของระบบ (system availability) รวมถึงจัดให้มีการติดตามและประเมินผล พร้อมทั้งรายงานผลให้คณะกรรมการทราบอย่างสม่ำเสมอ ตลอดจนเปิดเผยผลการดำเนินงานตามเป้าหมายในการให้บริการที่สำคัญให้สมาชิกทราบด้วย

5. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับนับแต่วันที่ 16 เมษายน 2561 เป็นต้นไป

ประกาศ ณ วันที่ เดือน พ.ศ.

(นายวิรไท สันติประภพ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายนโยบายระบบการชำระเงิน
โทรศัพท์ 0 2283 5096, 0 2283 5137