**(ร่าง) ประกาศธนาคารแห่งประเทศไทย**
**ที่ สกช.  /2568**
**เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่**

---

**1. เหตุผลในการออกประกาศ**

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology : IT) มีบทบาทสำคัญสำหรับการดำเนินธุรกิจของสถาบันการเงิน สถาบันการเงินเฉพาะกิจ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ โดยเฉพาะช่องทางการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (บริการ mobile banking) มีการใช้งานเพิ่มขึ้นอย่างรวดเร็ว และยังคงขยายตัวอย่างต่อเนื่อง ขณะเดียวกันการให้บริการผ่านช่องทางดังกล่าวก็นำมาซึ่งความเสี่ยงจากภัยคุกคามไซเบอร์ (cyber threat) และภัยทุจริตทางการเงิน (fraud) ธนาคารแห่งประเทศไทย (ธปท.) ตระหนักถึงความสำคัญในเรื่องดังกล่าว จึงได้ออกแนวนโยบายเรื่องการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ ในปี 2562 รวมทั้ง กำหนดมาตรการเพิ่มเติมเพื่อปิดความเสี่ยงจากภัยทุจริตทางการเงินที่มีการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (unauthorized payment fraud) ในปี 2566 อย่างไรก็ตาม ภัยคุกคามไซเบอร์และภัยทุจริตทางการเงิน unauthorized payment fraud มีการปรับเปลี่ยนรูปแบบและใช้เทคนิควิธีการที่ซับซ้อนมากขึ้น สร้างความเสียหายต่อผู้ใช้บริการในวงกว้าง ส่งผลกระทบต่อความน่าเชื่อถือของระบบสถาบันการเงินและระบบการชำระเงินของประเทศ

ธปท. จึงเห็นควรออกหลักเกณฑ์ การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ เพื่อให้บริการ mobile banking มีมาตรฐานขั้นต่ำที่จำเป็นสำหรับการให้บริการอย่างปลอดภัย เท่าทันความเสี่ยงจากภัยคุกคามไซเบอร์และ unauthorized payment fraud

**2. อำนาจตามกฎหมาย**

...

**3. ประกาศที่ยกเลิก**

...

**4. ขอบเขตการบังคับใช้**

ประกาศฉบับนี้ให้ใช้บังคับกับสถาบันการเงิน และสถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน ที่ให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ แก่ผู้ใช้บริการกลุ่มลูกค้ารายย่อย

**5. นิยาม**

ในประกาศฉบับนี้

“อุปกรณ์เคลื่อนที่” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์แบบพกพาซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่น เพื่อรับหรือส่งข้อมูลทางการเงิน การชำระเงิน หรือคำสั่งการชำระเงินผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง

“ผู้ให้บริการ” หมายความว่า สถาบันการเงินและสถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการทางการเงินและการชำระเงินโดยช่องทางการให้บริการผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่

“ภัยทุจริตทางการเงินที่มีการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (unauthorized payment fraud)” หมายถึง ภัยทุจริตที่เกิดขึ้นจากการที่ผู้ไม่ประสงค์ดีสวมรอยทำธุรกรรมแทนผู้ใช้บริการ โดยที่ผู้ใช้บริการไม่ได้ให้ความยินยอม เช่น กรณี ผู้ไม่ประสงค์ดีติดตั้ง malware บนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ ทำให้สามารถเข้าถึงหรือควบคุมอุปกรณ์เคลื่อนที่และแอปพลิเคชันและสวมรอยทำธุรกรรมผ่านบัญชีของผู้ใช้บริการโดยไม่ได้รับอนุญาต เป็นต้น

**6. หลักการ**

ผู้ให้บริการที่ให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่มีหน้าที่ติดตามดูแลและปรับปรุงระบบงานและบริการ mobile banking ให้มีความมั่นคงปลอดภัยตามมาตรฐานสากลเท่าทันภัยคุกคามไซเบอร์และภัยทุจริตรูปแบบใหม่ที่มีเทคนิคซับซ้อนขึ้น ครอบคลุมตั้งแต่การรักษาความมั่นคงปลอดภัยอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ ไปจนถึงระบบการให้บริการของผู้ให้บริการ

**7. หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่**

หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ ประกอบด้วยมาตรการ 2 ส่วน ได้แก่ (1) การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ และ (2) การรักษาความมั่นคงปลอดภัยของแอปพลิเคชัน mobile banking ดังนี้

**7.1 การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ**

ผู้ให้บริการต้องดำเนินการให้มีการป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการโดยอย่างน้อยต้องดำเนินการ ดังนี้

7.1.1 งดเว้นแนบลิงก์ผ่านช่องทางข้อความสั้น (SMS) และช่องทางอีเมล สำหรับกรณีช่องทางสื่อสังคมออนไลน์ (social media) งดเว้นแนบลิงก์เฉพาะที่เป็นการขอข้อมูลในการยืนยันตัวตนและข้อมูลส่วนบุคคลที่สำคัญ เช่น ชื่อผู้ใช้งาน รหัสผ่าน รหัสใช้ครั้งเดียว (one time password

: OTP) รหัส PIN หมายเลขบัตรประชาชนชน วันเดือนปีเกิด เป็นต้น เพื่อป้องกันการสวมรอยเป็นผู้ให้บริการ การขอให้เปิดเผยข้อมูลสำคัญ (social engineering) หรือการถูกติดตั้ง mobile malware ทั้งนี้ กรณีผู้ใช้บริการดำเนินการร้องขอเอง ผู้ให้บริการสามารถแนบลิงก์ได้เป็นรายครั้ง

7.1.2 ต้องมีกระบวนการติดตามแอปพลิเคชันที่ปลอมแปลงและแอบอ้างเป็นผู้ให้บริการผ่านช่องทางต่าง ๆ เช่น เว็บไซต์ สื่อสังคมออนไลน์ แพลตฟอร์มที่เป็นทางการ (official app store) เป็นต้น และหากพบว่าแอปพลิเคชันของผู้ให้บริการถูกปลอมแปลง ผู้ให้บริการต้องมีกระบวนการรับมืออย่างทันการณ์ เพื่อลดความเสี่ยงที่ผู้ใช้บริการหลงเชื่อเปิดเผยข้อมูลสำคัญ ถูกติดตั้ง malware หรือแอปพลิเคชันปลอม

7.1.3 จำกัดการใช้บริการ mobile banking ของผู้ใช้บริการเพียง 1 บัญชีผู้ใช้งาน และจำกัดให้ใช้งานบน 1 อุปกรณ์ของผู้ใช้บริการเท่านั้น

7.1.4 ต้องจัดให้มีการยืนยันตัวตนผู้ใช้บริการเพิ่มเติมในขั้นตอนการทำธุรกรรมผ่านอุปกรณ์เคลื่อนที่ โดยใช้เทคโนโลยีเปรียบเทียบใบหน้า (face recognition) ร่วมกับการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) เช่น การใช้เทคโนโลยี liveness detection เป็นต้น เพื่อให้เทคโนโลยีเปรียบเทียบใบหน้าสามารถป้องกันการใช้รูปภาพ วิดีโอ หรือการปลอมแปลงชีวมิติในรูปแบบต่าง ๆ ได้ เมื่อธุรกรรมดังกล่าวเป็นธุรกรรมที่เข้าเงื่อนไขอย่างใดอย่างหนึ่ง ดังนี้

(1) ทำธุรกรรมโอนเงินในแต่ละครั้งมีมูลค่า ตั้งแต่ 50,000 บาทขึ้นไป หรือ
(2) ทำธุรกรรมโอนเงินมูลค่ารวมกัน ครบทุก ๆ 200,000 บาท ในรอบระยะเวลา 1 วัน หรือ
(3) ปรับเพิ่มวงเงินการทำธุรกรรมโอนเงินต่อวัน ให้สามารถโอนได้ตั้งแต่ 50,000 บาท ขึ้นไป

ทั้งนี้ หากการทำธุรกรรมข้างต้นเป็นธุรกรรมที่มีความเสี่ยงต่ำ เช่น การทำธุรกรรมโอนเงินระหว่างบัญชีตนเอง การทำธุรกรรมโอนเงินประจำอัตโนมัติ (automatic recurring transfer) และได้ยืนยันตัวตนไปแล้วในครั้งแรก เป็นต้น อาจพิจารณางดเว้นการยืนยันตัวตนเพิ่มเติมตามที่กำหนดข้างต้น

7.1.5 กำหนดเพดานวงเงินสูงสุดต่อวันสำหรับธุรกรรมถอนเงินหรือโอนเงินผ่านบริการ mobile banking ให้เหมาะสมตามระดับเสี่ยงของกลุ่มผู้ใช้บริการแต่ละประเภท เพื่อลดความเสียหายเมื่อผู้ใช้บริการตกเป็นเหยื่อ หรือถูกใช้เป็นเครื่องมือในการทำทุจริต เช่น กรณีกลุ่มผู้ใช้บริการที่อายุต่ำกว่า 15 ปี ให้กำหนดวงเงินสูงสุดไม่เกิน 50,000 บาทต่อวัน เป็นต้น ทั้งนี้ ผู้ให้บริการควรนำแนวทางหรือข้อกำหนดที่ได้จัดทำร่วมกัน เช่น การจัดระดับความเสี่ยงบุคคลตามแนวปฏิบัติ ในการบริหารจัดการบัญชีเงินฝากที่ถูกใช้หรืออาจถูกใช้ทำธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี (industry standard) เป็นต้น มาใช้ประกอบการจัดระดับความเสี่ยงของกลุ่มผู้ใช้บริการด้วย

### 7.2 การรักษาความมั่นคงปลอดภัยของแอปพลิเคชัน mobile banking

ผู้ให้บริการต้องกำหนดให้มีการรักษาความมั่นคงปลอดภัยแอปพลิเคชันที่ให้บริการ mobile banking ภายใต้กรอบหลักการที่สำคัญ คือ (1) การรักษาความมั่นคงปลอดภัยข้อมูล (2) การรักษาความมั่นคงปลอดภัยแอปพลิเคชัน และ (3) การรักษาความมั่นคงปลอดภัยอุปกรณ์

เคลื่อนที่ เพื่อป้องกันความเสี่ยงจากภัยคุกคามไซเบอร์และภัยทุจริตทางการเงินที่ส่งผลกระทบต่อผู้ใช้บริการและความเชื่อมั่นต่อระบบสถาบันการเงิน ดังนี้

**7.2.1 การรักษาความมั่นคงปลอดภัยข้อมูล**

ผู้ให้บริการต้องรักษาความลับและความปลอดภัยของข้อมูลสำคัญของผู้ใช้บริการอย่างรัดกุม เพื่อป้องกันข้อมูลสำคัญของผู้ใช้บริการรั่วไหล หรือถูกเปลี่ยนแปลงแก้ไข ทั้งขณะจัดเก็บ แสดงผล และรับ-ส่งข้อมูลระหว่างอุปกรณ์เคลื่อนที่ของผู้ใช้บริการและระบบงานของผู้ให้บริการ โดยต้องดำเนินการอย่างน้อย ดังนี้

(1) หลีกเลี่ยงการจัดเก็บข้อมูลสำคัญไว้ในอุปกรณ์เคลื่อนที่ โดยหากจำเป็นต้องจัดเก็บข้อมูลดังกล่าว ต้องมีกระบวนการรักษาความปลอดภัยที่รัดกุม โดยอย่างน้อย ผู้ให้บริการต้องเข้ารหัสไฟล์ข้อมูล (files encryption) ด้วยวิธีการที่ปลอดภัยตามมาตรฐานสากล และทำลายข้อมูลเมื่อสิ้นสุดการใช้งานข้อมูล

(2) แอปพลิเคชันของผู้ให้บริการต้องแสดงผลข้อมูลสำคัญ (sensitive information) ของผู้ใช้บริการเท่าที่จำเป็นและเป็นไปอย่างรัดกุม โดยอย่างน้อย ต้องปิดบังการแสดงข้อมูลรหัสผ่าน และปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (application blurring)

(3) ใช้ช่องทางสื่อสารที่ปลอดภัย (secure protocol) และยืนยันตัวตนด้วยเทคนิค certificate pinning หรือวิธีอื่นที่เทียบเท่า รวมทั้งต้องดำเนินการเข้ารหัสข้อมูลสำคัญในระดับแอปพลิเคชัน (application layer) ในการรับ-ส่งข้อมูล เพื่อป้องกันการถูกดักจับหรือแก้ไขเปลี่ยนแปลงข้อมูลระหว่างการรับส่ง (man in the middle attack)

**7.2.2 การรักษาความมั่นคงปลอดภัยแอปพลิเคชัน**

ผู้ให้บริการต้องติดตามดูแลและปรับปรุงแอปพลิเคชันให้มีความมั่นคงปลอดภัยตามมาตรฐานสากล เท่าทันภัยคุกคามรูปแบบใหม่อยู่เสมอ โดยต้องดำเนินการอย่างน้อย ดังนี้

(1) แอปพลิเคชันของผู้ให้บริการต้องขอสิทธิ์เข้าถึงทรัพยากรหรือบริการบนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ (application permission) เท่าที่จำเป็น และมีกระบวนการทบทวนการขอสิทธิ์ดังกล่าวอย่างเป็นประจำ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อป้องกันการละเมิดสิทธิ์ความเป็นส่วนตัวของผู้ใช้บริการและถูกใช้เป็นช่องโหว่โดยผู้ไม่ประสงค์ดี

(2) ไม่ให้บริการแอปพลิเคชันในเวอร์ชันที่มีช่องโหว่ซึ่งยังไม่ได้ถูกแก้ไข และอาจทำให้เกิดความเสี่ยง unauthorized payment fraud ต่อผู้ใช้บริการ

(3) ตรวจสอบการเปลี่ยนแปลงแก้ไขแอปพลิเคชัน เมื่อผู้ใช้บริการเข้าใช้งานในทันที (anti-tampering) และไม่อนุญาตให้ผู้ใช้บริการใช้งานแอปพลิเคชันที่ถูกเปลี่ยนแปลงแก้ไข เพื่อป้องกันไม่ให้ข้อมูลผู้ใช้บริการรั่วไหลหรือเกิดความเสียหายจากแอปพลิเคชันที่มีการดัดแปลงแก้ไข เช่น ฝัง malicious code เป็นต้น

(4) จัดการ session อย่างปลอดภัย เพื่อป้องกันการสวมรอยเข้าใช้งานโดยไม่ได้รับอนุญาต (session hijacking)

(5) ป้องกัน source code ของแอปพลิเคชันถูกเปิดเผยต่อสาธารณะ เช่น การทำ source code obfuscation เป็นต้น เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีสามารถเข้าถึง source code และอาจเป็นเหตุให้สามารถทำการเปลี่ยนแปลงแก้ไข source code ได้

**7.2.3 การรักษาความมั่นคงปลอดภัยอุปกรณ์เคลื่อนที่**

ผู้ให้บริการต้องให้บริการ mobile banking ในสภาพแวดล้อมของอุปกรณ์เคลื่อนที่ที่ปลอดภัย เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีอาศัยช่องโหว่ของระบบปฏิบัติการ เข้าถึง mobile banking และบัญชีของผู้ใช้บริการ โดยต้องดำเนินการอย่างน้อย ดังนี้

(1) ไม่อนุญาตให้แอปพลิเคชันของผู้ให้บริการใช้งานบนอุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการล้าสมัย (obsolete Operating System : OS) และมีช่องโหว่ที่อาจทำให้เกิด unauthorized payment fraud

(2) ไม่อนุญาตให้แอปพลิเคชันของผู้ให้บริการใช้งานบนอุปกรณ์เคลื่อนที่ที่เปิดสิทธิ์ให้เข้าถึงระบบปฏิบัติการ (rooted/jailbroken)

(3) ไม่อนุญาตให้แอปพลิเคชันของผู้ให้บริการใช้งานบนอุปกรณ์เคลื่อนที่ที่ติดตั้งแอปพลิเคชันอื่นที่มีพฤติกรรมการทำงานที่ต้องสงสัย เช่น แอปพลิเคชันที่ขอสิทธิ์ช่วยเหลือคนพิการ (accessibility services) โดยไม่จำเป็น แอปพลิเคชันที่สามารถควบคุมอุปกรณ์เคลื่อนที่จากระยะไกลได้ (remote control) แอปพลิเคชันที่มีการปิดบังหรือขโมยข้อมูลที่แสดงบนหน้าจอของผู้ใช้งาน เป็นต้น เพื่อลดความเสี่ยงที่แอปพลิเคชันของผู้ให้บริการถูกควบคุมหรือเข้าถึงโดย malware ที่มีการติดตั้งบนอุปกรณ์เคลื่อนที่

ทั้งนี้ ผู้ให้บริการต้องติดตาม และปรับปรุงการรักษาความมั่นคงปลอดภัยของการให้บริการ mobile banking ให้เท่าทันภัยคุกคามไซเบอร์และภัยทุจริตรูปแบบใหม่ เป็นไปตามมาตรฐานสากลอย่างต่อเนื่อง โดยกรณีที่พบช่องโหว่ใหม่ ผู้ให้บริการต้องเร่งดำเนินการให้มีแนวทางป้องกัน เพื่อปิดช่องโหว่ภายในกรอบเวลาที่เหมาะสม หรือดำเนินการให้แล้วเสร็จภายในระยะเวลาที่ ธปท. กำหนด

**8. การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์**

กรณีที่ผู้ให้บริการมีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ได้ ให้ยื่นขอผ่อนผันเป็นรายกรณีต่อ ธปท. พร้อมแสดงเหตุผลและความจำเป็น รวมถึงแผนการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธปท. จะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน โดย ธปท. อาจจะพิจารณาอนุญาตหรือไม่ก็ได้ หรือกำหนดเงื่อนไขใด ๆ ให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

**9. บทเฉพาะกาล**

ผู้ให้บริการที่มีการให้บริการ mobile banking ก่อนวันที่ประกาศฉบับนี้มีผลใช้บังคับ ให้ดำเนินการปรับปรุงระบบให้เป็นไปตามประกาศ ภายในวันที่ ...

**10. วันเริ่มต้นบังคับใช้**

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ มกราคม 2568

(นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์