ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Consultation Paper

เอกสารรับฟังความคิดเห็น

หลักการของการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินผ่านช่องทางดิจิทัล

(Digital Channel Security)

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สายกำกับระบบการชำระเงินและคุ้มครองผู้ใช้บริการทางการเงิน
ธนาคารแห่งประเทศไทย

กรกฎาคม 2569

บทนำ

การให้บริการทางการเงินผ่านช่องทางดิจิทัลมีการใช้งานเพิ่มขึ้นอย่างรวดเร็ว ขณะเดียวกันบริการดังกล่าวก็นำมาซึ่งความเสี่ยงจากภัยคุกคามทางไซเบอร์ (cyber threat) และภัยทุจริตทางการเงินที่มีการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (unauthorized payment fraud) ได้

ที่ผ่านมา ธนาคารแห่งประเทศไทย (ธปท.) ตระหนักถึงความสำคัญในการป้องกันภัยดังกล่าว จึงได้ออกประกาศหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Mobile Banking Security) เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำที่จำเป็นสำหรับการให้บริการ Mobile Banking ของสถาบันการเงิน สถาบันการเงินเฉพาะกิจ และผู้ให้บริการ e-Money ส่งผลให้ภัยทุจริตในรูปแบบแอปดูดเงินลดลงอย่างมีนัยสำคัญในปี 2567 อย่างไรก็ตาม มิจฉาชีพเริ่มเปลี่ยนเป้าหมายการโจมตีไปยังผู้ให้บริการทางการเงินที่มิใช่สถาบันการเงิน เช่น การสวมรอยทำธุรกรรมบนแอปพลิเคชันบัตรเครดิต และเบิกถอนเงินสดทางตู้ ATM ผ่านบริการถอนเงินไม่ใช้บัตร (cardless withdrawal) รวมทั้งใช้เทคนิควิธีการที่มีความซับซ้อนมากขึ้น เช่น การติดตั้งมัลแวร์บนเครื่องคอมพิวเตอร์เหยื่อเพื่อดักจับรหัสผ่านและ SMS OTP สำหรับเข้าใช้บริการ Internet Banking เป็นต้น

ธปท. จึงเห็นควรออกประกาศหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินผ่านช่องทางดิจิทัล (Digital Channel Security) เพื่อยกระดับการรักษาความมั่นคงปลอดภัยของบริการทางการเงินผ่านช่องทางดิจิทัล ได้แก่ บริการทางการเงินผ่าน Mobile Application และบริการ Internet Banking ให้เท่าทันภัยคุกคามทางไซเบอร์และภัยทุจริต unauthorized payment fraud ตลอดจนสร้างความเชื่อมั่นในระบบสถาบันการเงินและระบบการชำระเงินของประเทศ

ธปท. จึงได้จัดทำเอกสารรับฟังความคิดเห็นฉบับนี้ เพื่อรับฟังความคิดเห็นและข้อเสนอแนะจากผู้ที่เกี่ยวข้องอย่างรอบด้าน เพื่อนำมาประกอบการพิจารณาออกหลักเกณฑ์ฯ ให้เหมาะสมต่อไป ธปท. ขอเชิญทุกท่านร่วมแสดงความคิดเห็นและข้อเสนอแนะต่อร่างหลักเกณฑ์ฉบับนี้ ตั้งแต่วันที่ 23 กรกฎาคม - 24 สิงหาคม 2569

หลักการ

ผู้ให้บริการทางการเงินที่ให้บริการผ่านช่องทางดิจิทัลมีหน้าที่ติดตามและดูแลให้บริการมีความมั่นคงปลอดภัยสอดคล้องตามมาตรฐานสากล เท่าทันภัยคุกคามทางไซเบอร์และภัยทุจริต unauthorize payment fraud ดังนี้

1. **ขอบเขตการบังคับใช้** ครอบคลุม สถาบันการเงิน สถาบันการเงินเฉพาะกิจ (SFI) ผู้ให้บริการ e-Money ผู้ให้บริการบัตรเครดิตและสินเชื่อ ที่ให้บริการโอนเงินไปยังบุคคลอื่นที่มีอยู่กับผู้ให้บริการทางการเงินอื่น หรือให้บริการถอนเงินสดกับลูกค้าบุคคลธรรมดาผ่านช่องทาง Mobile Application และ Internet Banking
2. **มาตรการยืนยันตัวตนลูกค้าอย่างปลอดภัย (Authentication)** ผู้ให้บริการทางการเงินต้องยกระดับการยืนยันตัวตนของลูกค้าในขั้นตอนที่มีความสำคัญโดยแบ่งมาตรการออกเป็น 3 เรื่อง ดังนี้
   - **2.1. ขั้นตอนการสมัครบริการ หรือเปลี่ยนอุปกรณ์เคลื่อนที่:** ผู้ให้บริการทางการเงินต้องจัดให้มีการพิสูจน์ยืนยันตัวตนลูกค้าอย่างรัดกุม เพื่อให้มั่นใจว่าผู้สมัครใช้บริการเป็นลูกค้าตัวจริง รวมทั้งแจ้งผลการสมัครใช้บริการไปยังลูกค้าทันทีผ่านช่องทางอื่น (Out-of-Band Notification) เช่น LINE Official Account โทรศัพท์ หรืออีเมล เป็นต้น นอกจากนี้ ต้องจัดให้มีมาตรการลดความเสี่ยงลูกค้าในช่วงแรกหลังการสมัครบริการหรือเปลี่ยนอุปกรณ์ เช่น การจำกัดการใช้บริการชั่วคราวหลังสมัครบริการ (Cooling-off Period) การจำกัดให้ทำได้เฉพาะธุรกรรมเสี่ยงต่ำ การจำกัดวงเงินขั้นต่ำชั่วคราว เป็นต้น เพื่อจำกัดความเสียหายในกรณีที่เกิดการถูกสวมรอยสมัครใช้บริการ
   - **2.2. ขั้นตอนการทำธุรกรรม:** ผู้ให้บริการทางการเงินต้องใช้วิธีการยืนยันตัวตนลูกค้าแบบ 2 ขั้นตอนที่เป็นอิสระต่อกัน (Two-Factor Authentication: MFA) อย่างน้อยครอบคลุมขั้นตอนโอนเงิน การสร้างรายการถอนเงินผ่าน Mobile Application และรับเงินที่ตู้ ATM และการเพิ่มวงเงินสำหรับทำธุรกรรม
   - **2.3. ปัจจัยยืนยันตัวตนที่ปลอดภัย:** ผู้ให้บริการทางการเงินต้องเลือกใช้ปัจจัยยืนยันตัวตนที่ปลอดภัย ยากต่อการถูกปลอมแปลง ทบทวนและปรับปรุงปัจจัยยืนยันตัวตนให้มีความปลอดภัยเท่าทันรูปแบบภัยคุกคามใหม่อยู่เสมอ โดยกรณี ปัจจัยประเภท What-you-know ต้องสามารถป้องกันการสุ่มเดารหัสผ่านทุกความเป็นไปได้ (Brute Force attack) ปัจจัยประเภท What-you-have ต้องใช้ปัจจัยที่มีความปลอดภัย เช่น Mobile Application ที่ผ่านการลงทะเบียนกับผู้ให้บริการทางการเงิน (device binding) หรือ Hard/Soft Token และยกเลิกการใช้รหัสผ่านครั้งเดียว (OTP) ผ่านช่องทาง SMS สำหรับยืนยันตัวตนในการทำธุรกรรม และปัจจัยประเภท What you are เช่น การสแกนใบหน้าต้องใช้เทคโนโลยีที่มีความแม่นยำและมีประสิทธิภาพในการตรวจจับการปลอมแปลงอัตลักษณ์ โดยปฏิบัติตาม

มาตรฐานของแนวปฏิบัติ ธปท. เรื่องการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน

3. **มาตรการป้องกันการสวมรอยเป็นผู้ให้บริการ** เพื่อป้องกันมิจฉาชีพแอบอ้างหรือสวมรอยเป็นผู้ให้บริการทางการเงิน โดยให้ผู้ให้บริการทางการเงินต้องงดเว้นการส่ง SMS และอีเมลแนบ Link รวมทั้ง มีกระบวนการรับมือและตอบสนองหากพบการปลอมแปลง Application หรือ Website ของผู้ให้บริการ
4. **มาตรการรักษาความปลอดภัยบริการผ่านช่องทาง Mobile Application** ผู้ให้บริการทางการเงินที่มีการให้บริการผ่านช่องทาง Mobile Application ต้องมีการรักษาความปลอดภัย Mobile Application และการควบคุมสภาพแวดล้อมของอุปกรณ์เคลื่อนที่ที่ติดตั้งแอปพลิเคชันของผู้ใช้งาน เพื่อให้มั่นใจว่าแอปพลิเคชันของผู้ให้บริการทำงานได้อย่างปลอดภัย เช่น การป้องกันการเปลี่ยนแปลงแก้ไขแอปพลิเคชัน การป้องกันแอปพลิเคชันรีโมท เป็นต้น รวมทั้ง การทำธุรกรรมมูลค่าสูงต้องมีการพิสูจน์ตัวตนด้วยการใช้เทคโนโลยีเปรียบเทียบใบหน้า ร่วมกับการตรวจจับการปลอมแปลงชีวมิติเพิ่มเติม เช่น การสแกนใบหน้าเมื่อโอนเงินเกิน 50,000 บาทต่อครั้ง หรือ 200,000 บาทต่อวัน เป็นต้น