ธนาคารแห่งประเทศไทย

10 กุมภาพันธ์ 2568

เรียน ผู้จัดการ
สถาบันการเงินทุกแห่ง

ที่ ธปท.ว.1218/2568 เรื่อง นำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงิน

ธนาคารแห่งประเทศไทย (ธปท.) ขอนำส่งประกาศธนาคารแห่งประเทศไทย ที่ 4/2568 เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงิน (ประกาศฯ) ซึ่งได้ประกาศลงในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 142 ตอนพิเศษ 55 ง วันที่ 7 กุมภาพันธ์ 2568 แล้ว และมีผลบังคับใช้เมื่อพ้นกำหนด 30 วัน นับแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป ยกเว้นประกาศฯ ข้อ 5.3.2 (3.3) มีผลบังคับใช้เมื่อพ้นกำหนด 60 วันนับแต่วันถัดจากประกาศในราชกิจจานุเบกษาเป็นต้นไป

สาระสำคัญของการออกประกาศฯ เพื่อเป็นการยกระดับการให้บริการ Mobile Banking ให้มีมาตรฐานขั้นต่ำที่จำเป็นสำหรับการให้บริการทางการเงินและการชำระเงินบนแอปพลิเคชันของสถาบันการเงินอย่างปลอดภัย โดยสถาบันการเงินมีหน้าที่ต้องติดตามดูแล และปรับปรุงระบบงานและบริการ Mobile Banking ให้มีความมั่นคงปลอดภัยตามมาตรฐานสากล เท่าทันภัยคุกคามทางไซเบอร์และภัยทุจริตรูปแบบใหม่ที่มีเทคนิคซับซ้อนขึ้น ครอบคลุมทั้งในส่วนของระบบการให้บริการของสถาบันการเงิน และความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นางสาวโรรา อุนนะนันทน์)
ผู้อำนวยการอาวุโส ฝ่ายกำกับและตรวจสอบความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย ประกาศธนาคารแห่งประเทศไทย ที่ 4/2568 เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงิน

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6347, 0 2283 6364
ไปรษณีย์อิเล็กทรอนิกส์ ITSupervision@bot.or.th

หมายเหตุ [X] ธปท. จัดประชุมชี้แจงเมื่อวันที่ 17 ธันวาคม 2567
[ ] ไม่มีการประชุมชี้แจง

ประกาศธนาคารแห่งประเทศไทย

ที่ 4 /2568

เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงิน

---

1. เหตุผลในการออกประกาศ

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology : IT) มีบทบาทสำคัญสำหรับการดำเนินธุรกิจของสถาบันการเงิน โดยเฉพาะการให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันของสถาบันการเงินแก่ผู้ใช้บริการที่เป็นบุคคลธรรมดาบนอุปกรณ์เคลื่อนที่ (บริการ Mobile Banking) ที่มีการใช้งานเพิ่มขึ้นอย่างรวดเร็ว และยังคงขยายตัวอย่างต่อเนื่อง ขณะเดียวกันการให้บริการ Mobile Banking ก็นำมาซึ่งความเสี่ยงจากภัยคุกคามทางไซเบอร์ (cyber threat) และภัยทุจริตทางการเงิน (fraud) ที่มีการปรับเปลี่ยนรูปแบบและใช้เทคนิควิธีการที่ซับซ้อนมากขึ้น อันอาจสร้างความเสียหายต่อผู้ใช้บริการในวงกว้าง ส่งผลกระทบต่อความน่าเชื่อถือของระบบสถาบันการเงินและระบบการชำระเงินของประเทศ

ธนาคารแห่งประเทศไทยตระหนักถึงความสำคัญในการป้องกันภัยทุจริตดังกล่าว จึงได้ออกประกาศหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ เพื่อยกระดับการให้บริการ Mobile Banking ให้มีมาตรฐานขั้นต่ำที่จำเป็นสำหรับการให้บริการทางการเงินและการชำระเงินบนแอปพลิเคชันของสถาบันการเงินให้เป็นไปอย่างปลอดภัย เท่าทันความเสี่ยงจากภัยคุกคามทางไซเบอร์และภัยทุจริตทางการเงินที่มีการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (Unauthorized Payment Fraud)

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 39 และมาตรา 41 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

3. แนวนโยบายที่ยกเลิก

3.1 แนวนโยบาย เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ตามหนังสือเวียนธนาคารแห่งประเทศไทย ที่ ธปท.ฝตท.(01) ว. 1922/2562 ลงวันที่ 27 ธันวาคม 2562

3.2 ข้อ 1.2 ข้อ 1.4 และข้อ 1.6 ในเอกสารแนบ 2 ของแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ฉบับลงวันที่ 29 มีนาคม 2566

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

5. เนื้อหา

5.1 คำจำกัดความ

ในประกาศฉบับนี้

“อุปกรณ์เคลื่อนที่” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์แบบพกพาซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่น เพื่อรับหรือส่งข้อมูลทางการเงิน การชำระเงิน หรือคำสั่งการชำระเงินผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง

“สถาบันการเงิน” หมายความว่า สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“ผู้ใช้บริการ” หมายความว่า บุคคลธรรมดาที่ใช้บริการทางการเงินและการชำระเงินผ่านบริการ Mobile Banking บนอุปกรณ์เคลื่อนที่

“บริการ Mobile Banking” หมายความว่า การให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันของสถาบันการเงินที่มีการให้บริการแก่ผู้ใช้บริการบนอุปกรณ์เคลื่อนที่ซึ่งให้บริการถอนเงิน โอนเงิน หรือการชำระค่าสินค้าและบริการ อย่างใดอย่างหนึ่ง

“การสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (Unauthorized Payment Fraud)” หมายถึง ภัยทุจริตทางการเงินที่เกิดขึ้นจากการที่ผู้อื่นสวมรอยทำธุรกรรมแทนผู้ใช้บริการโดยทุจริตโดยที่ผู้ใช้บริการไม่ได้ให้ความยินยอม เช่น กรณีผู้ไม่ประสงค์ดีติดตั้ง malware บนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ ทำให้สามารถเข้าถึงหรือควบคุมอุปกรณ์เคลื่อนที่และแอปพลิเคชัน และสวมรอยทำธุรกรรมผ่านบัญชีของผู้ใช้บริการโดยไม่ได้รับอนุญาต

5.2 หลักการ

สถาบันการเงินที่ให้บริการ Mobile Banking บนอุปกรณ์เคลื่อนที่มีหน้าที่ต้องติดตามดูแลและปรับปรุงระบบงานและบริการ Mobile Banking ให้มีความมั่นคงปลอดภัยตามมาตรฐานสากลเท่าทันภัยคุกคามทางไซเบอร์และภัยทุจริตรูปแบบใหม่ที่มีเทคนิคซับซ้อนขึ้น ครอบคลุมทั้งในส่วนของระบบการให้บริการของสถาบันการเงิน และความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ

5.3 หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่

หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ ประกอบด้วยมาตรการ 2 ส่วน ได้แก่ (1) การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (Unauthorized Payment Fraud) และ (2) การรักษาความมั่นคงปลอดภัยของบริการ Mobile Banking ดังนี้

5.3.1 การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ

สถาบันการเงินต้องมีการป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ โดยอย่างน้อยต้องดำเนินการ ดังต่อไปนี้

(1) งดเว้นการแนบลิงก์ผ่านช่องทางข้อความสั้น (SMS) และช่องทางอีเมล แต่สำหรับกรณีช่องทางสื่อสังคมออนไลน์ (social media) ให้สถาบันการเงินงดแนบลิงก์เฉพาะที่มีการขอข้อมูลในการยืนยันตัวตน หรือข้อมูลส่วนบุคคล เช่น ชื่อผู้ใช้งาน รหัสผ่าน รหัสใช้ครั้งเดียว (one time password - OTP) รหัส PIN หมายเลขบัตรประชาชนชน วันเดือนปีเกิด เพื่อป้องกันการสวมรอยเป็นสถาบันการเงิน การขอให้เปิดเผยข้อมูลสำคัญ (social engineering) หรือการถูกติดตั้ง mobile malware

อย่างไรก็ดี สถาบันการเงินสามารถแนบลิงก์ผ่านทั้ง 3 ช่องทางดังกล่าวได้ หากผู้ใช้บริการดำเนินการร้องขอเอง โดยสถาบันการเงินสามารถแนบลิงก์ได้เป็นรายครั้ง พร้อมทั้งต้องมีการสื่อสารย้ำให้ผู้ใช้บริการทราบว่าการส่งลิงก์ดังกล่าวเป็นกรณีเฉพาะตามคำร้องขอของผู้ใช้บริการเป็นรายครั้งเท่านั้น

(2) มีกระบวนการติดตามและรับมืออย่างทันการณ์ต่อแอปพลิเคชันที่ปลอมแปลงหรือแอบอ้างเป็นแอปพลิเคชันของสถาบันการเงินที่ให้บริการ Mobile Banking ในแพลตฟอร์มที่เป็นทางการของผู้ให้บริการดาวน์โหลดแอปพลิเคชัน (official app store) เช่น Google Play Store Apple App Store รวมทั้งมีกระบวนการรับมือและตอบสนองอย่างเหมาะสมและทันการณ์สำหรับแอปพลิเคชันปลอมแปลงที่อยู่นอกแพลตฟอร์มดังกล่าว เพื่อลดความเสี่ยงที่ผู้ใช้บริการจะหลงเชื่อและเปิดเผยข้อมูลสำคัญ ถูกติดตั้ง malware หรือถูกติดตั้งแอปพลิเคชันปลอม

(3) จำกัดการใช้บริการ Mobile Banking ของผู้ใช้บริการไว้เพียง 1 บัญชีผู้ใช้งานต่อ 1 บริการ Mobile Banking ของแต่ละสถาบันการเงิน และจำกัดการใช้บริการดังกล่าวโดยให้ใช้งานบน 1 อุปกรณ์เคลื่อนที่ของผู้ใช้บริการเท่านั้น

(4) ต้องจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้บริการเพิ่มเติมในขั้นตอนการทำธุรกรรมผ่านบริการ Mobile Banking บนอุปกรณ์เคลื่อนที่ โดยใช้เทคโนโลยีเปรียบเทียบใบหน้า (face comparison) ร่วมกับการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) ที่สามารถป้องกันการใช้รูปภาพ วิดีโอ หรือการปลอมแปลงชีวมิติในรูปแบบต่าง ๆ ได้ เช่น การใช้เทคโนโลยี liveness detection เพื่อให้มั่นใจว่าผู้ใช้บริการเป็นผู้ทำธุรกรรมด้วยตนเอง ซึ่งต้องจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้บริการเพิ่มเติมดังกล่าวอย่างน้อยในกรณีดังต่อไปนี้

(4.1) การทำธุรกรรมโอนเงินในแต่ละครั้งมีมูลค่าตั้งแต่ 50,000 บาทขึ้นไป หรือ

(4.2) การทำธุรกรรมโอนเงินมูลค่ารวมกัน ครบทุก 200,000 บาท ในรอบระยะเวลา 1 วัน หรือ

(4.3) การปรับเพิ่มวงเงินการทำธุรกรรมโอนเงินต่อวัน ให้สามารถโอนได้ตั้งแต่ 50,000 บาทขึ้นไป

ทั้งนี้ กรณีที่ผู้ใช้บริการมีข้อจำกัดในการใช้เทคโนโลยีเปรียบเทียบใบหน้า (face comparison) เช่น เป็นคนพิการทางสายตา สถาบันการเงินอาจพิจารณางดเว้นการยืนยันตัวตนเพิ่มเติมตามที่กำหนดข้างต้นได้ โดยต้องมีแนวทางลดความเสี่ยงทดแทน หรือกรณีการทำธุรกรรมที่มีความเสี่ยงต่ำ เช่น การทำธุรกรรมโอนเงินระหว่างบัญชีตนเอง การทำธุรกรรมโอนเงินประจำอัตโนมัติ (automatic recurring transfer) ที่ได้ยืนยันตัวตนไปแล้วในครั้งแรก สถาบันการเงินอาจพิจารณางดเว้นการยืนยันตัวตนเพิ่มเติมตามที่กำหนดข้างต้นได้

(5) กำหนดเพดานวงเงินสูงสุดต่อวันสำหรับธุรกรรมถอนเงินหรือโอนเงินผ่านบริการ Mobile Banking ให้เหมาะสมกับระดับความเสี่ยงของกลุ่มผู้ใช้บริการ เพื่อลดความเสียหายเมื่อผู้ใช้บริการตกเป็นเหยื่อ หรือถูกใช้เป็นเครื่องมือในการทุจริต เช่น กรณีกลุ่มผู้ใช้บริการที่อายุต่ำกว่า 15 ปี ให้กำหนดวงเงินสูงสุดของการทำธุรกรรมถอนหรือโอนเงินรวมกันไม่เกิน 50,000 บาทต่อวัน เป็นต้น

ทั้งนี้ สถาบันการเงินสามารถใช้แนวทางหรือข้อกำหนดที่ได้จัดทำร่วมกัน (industry standard) มาใช้ประกอบการจัดระดับความเสี่ยง หรือกำหนดเพดานวงเงินสูงสุดของกลุ่มผู้ใช้บริการได้ และในกรณีที่ผู้ใช้บริการขอยกเว้นการกำหนดวงเงินตามกลุ่มความเสี่ยงที่กำหนดไว้ สถาบันการเงินต้องมีกระบวนการพิจารณาการขอยกเว้นที่ชัดเจนและรัดกุมด้วย

5.3.2 การรักษาความมั่นคงปลอดภัยของบริการ Mobile Banking

สถาบันการเงินต้องกำหนดให้มีการรักษาความมั่นคงปลอดภัยแอปพลิเคชันที่ให้บริการ Mobile Banking ภายใต้กรอบหลักการที่สำคัญ คือ (1) การรักษาความมั่นคงปลอดภัยของข้อมูล (2) การรักษาความมั่นคงปลอดภัยของแอปพลิเคชัน และ (3) การรักษาความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่ เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์และภัยทุจริตทางการเงินที่ส่งผลกระทบต่อผู้ใช้บริการและความเชื่อมั่นต่อระบบสถาบันการเงิน ดังนี้

(1) การรักษาความมั่นคงปลอดภัยของข้อมูล

สถาบันการเงินต้องรักษาความลับและความปลอดภัยของข้อมูลสำคัญของผู้ใช้บริการอย่างรัดกุม เพื่อป้องกันข้อมูลสำคัญของผู้ใช้บริการรั่วไหล หรือถูกเปลี่ยนแปลงแก้ไขทั้งขณะจัดเก็บ แสดงผล และรับ-ส่งข้อมูลระหว่างอุปกรณ์เคลื่อนที่ของผู้ใช้บริการและระบบงานของสถาบันการเงิน โดยต้องดำเนินการอย่างน้อย ดังนี้

(1.1) หลีกเลี่ยงการจัดเก็บข้อมูลสำคัญไว้ในอุปกรณ์เคลื่อนที่ เช่น ข้อมูลที่ใช้ยืนยันตัวตน ข้อมูลส่วนบุคคล โดยหากจำเป็นต้องจัดเก็บข้อมูลดังกล่าว ต้องมีกระบวนการรักษาความปลอดภัยที่รัดกุม โดยอย่างน้อยสถาบันการเงินต้องเข้ารหัสข้อมูล (data encryption) ด้วยวิธีการที่ปลอดภัยตามมาตรฐานสากล และทำลายข้อมูลเมื่อสิ้นสุดการใช้งานข้อมูล

(1.2) แอปพลิเคชันของสถาบันการเงินต้องแสดงผลข้อมูลสำคัญ (sensitive information) ของผู้ใช้บริการเท่าที่จำเป็นและเป็นไปอย่างรัดกุม โดยอย่างน้อยต้องปิดบังการแสดงข้อมูลรหัสผ่าน และปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (application blurring)

(1.3) ใช้ช่องทางสื่อสารที่ปลอดภัย (secure protocol) และยืนยันตัวตนด้วยเทคนิค certificate pinning หรือวิธีอื่นที่เทียบเท่า รวมทั้งต้องดำเนินการเข้ารหัสข้อมูลสำคัญ

ในระดับแอปพลิเคชัน (application layer) ในการรับ-ส่งข้อมูล เพื่อป้องกันการถูกดักจับหรือแก้ไขเปลี่ยนแปลงข้อมูลระหว่างการรับส่ง (man in the middle attack)

(2) การรักษาความมั่นคงปลอดภัยของแอปพลิเคชัน

สถาบันการเงินต้องติดตามดูแลและปรับปรุงแอปพลิเคชันให้มีความมั่นคงปลอดภัยตามมาตรฐานสากลและเท่าทันภัยคุกคามรูปแบบใหม่อยู่เสมอ โดยต้องดำเนินการอย่างน้อยดังนี้

(2.1) แอปพลิเคชันของสถาบันการเงินต้องขอสิทธิเข้าถึงทรัพยากรหรือบริการบนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ (application permission) เท่าที่จำเป็น และมีการทบทวนการขอสิทธิดังกล่าวทุกครั้งที่มีการเปลี่ยนแปลงแอปพลิเคชันอย่างมีนัยสำคัญ เพื่อป้องกันการละเมิดสิทธิความเป็นส่วนตัวของผู้ใช้บริการ รวมถึงเป็นช่องโหว่ที่อาจถูกใช้โดยผู้อื่นที่กระทำการโดยทุจริต

(2.2) ไม่ให้บริการบนแอปพลิเคชันเวอร์ชันเก่าที่อาจมีช่องโหว่ และอาจทำให้เกิดความเสี่ยงในการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ

(2.3) ตรวจสอบการเปลี่ยนแปลงแก้ไขแอปพลิเคชันทุกครั้งในทันทีที่ผู้ใช้บริการเข้าใช้งาน (anti-tampering) และไม่อนุญาตให้ผู้ใช้บริการใช้งานแอปพลิเคชันที่ถูกเปลี่ยนแปลงแก้ไขเพื่อป้องกันไม่ให้ข้อมูลผู้ใช้บริการรั่วไหลหรือเกิดความเสียหายจากแอปพลิเคชันที่มีการดัดแปลงแก้ไข เช่น การฝัง malicious code

(2.4) จัดการการเชื่อมต่อระหว่างคอมพิวเตอร์ (session) ให้ปลอดภัยเพื่อป้องกันการสวมรอยเข้าใช้งานโดยไม่ได้รับอนุญาต (session hijacking)

(2.5) ป้องกัน source code ของแอปพลิเคชันไม่ให้อยู่ในรูปแบบที่อ่านเข้าใจโดยง่าย เช่น การทำ source code obfuscation เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงและทำการเปลี่ยนแปลงแก้ไข source code ได้

(3) การรักษาความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่

สถาบันการเงินต้องให้บริการ Mobile Banking ในสภาพแวดล้อมของอุปกรณ์เคลื่อนที่ที่ปลอดภัย เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีกระทำการทุจริตโดยอาศัยช่องโหว่ของระบบปฏิบัติการเข้าถึง Mobile Banking และบัญชีของผู้ใช้บริการ โดยต้องดำเนินการอย่างน้อย ดังนี้

(3.1) ไม่อนุญาตให้แอปพลิเคชันของสถาบันการเงินใช้งานบนอุปกรณ์เคลื่อนที่ที่ตรวจพบว่ามีการเปิดสิทธิให้เข้าถึงระบบปฏิบัติการ (rooted/jailbroken)

(3.2) ไม่อนุญาตให้แอปพลิเคชันของสถาบันการเงินทำงานบนอุปกรณ์เคลื่อนที่ในขณะที่มีแอปพลิเคชันอื่นกำลังทำงานและมีพฤติกรรมการทำงานที่เสี่ยงจะก่อให้เกิดการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ เช่น แอปพลิเคชันที่ขอสิทธิช่วยเหลือคนพิการ (accessibility services) โดยไม่จำเป็น แอปพลิเคชันที่สามารถควบคุมอุปกรณ์เคลื่อนที่จากระยะไกลได้ (remote control) แอปพลิเคชันที่มีการปิดบังหรือขโมยข้อมูลที่แสดงบนหน้าจอของผู้ใช้งาน เพื่อลดความเสี่ยงที่แอปพลิเคชันของสถาบันการเงินจะถูกควบคุมหรือเข้าถึงโดย malware ที่มีการติดตั้งบนอุปกรณ์เคลื่อนที่

(3.3) หลีกเลี่ยงการให้บริการ Mobile Banking ของสถาบันการเงินบนอุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการที่หน่วยงานด้านความมั่นคงปลอดภัยที่เป็นที่ยอมรับ เช่น Thailand Banking Sector Computer Emergency Response Team (TB-CERT) กำหนดว่ามีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ หรือการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ

กรณีสถาบันการเงินมีการให้บริการบนอุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการที่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ หรือการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ สถาบันการเงินต้องจัดให้มีแนวทางการควบคุมความเสี่ยงเพิ่มเติม โดยการแจ้งเตือนถึงความเสี่ยงจากกรณีดังกล่าว รวมทั้งจำกัดวงเงินการทำธุรกรรมของกลุ่มผู้ใช้บริการดังกล่าวให้ทำธุรกรรมโอนเงินได้ไม่เกินวันละ 5,000 บาท

ทั้งนี้ สถาบันการเงินต้องติดตามและปรับปรุงการรักษาความมั่นคงปลอดภัยของการให้บริการ Mobile Banking ให้เท่าทันภัยคุกคามทางไซเบอร์และภัยทุจริตรูปแบบใหม่ เป็นไปตามมาตรฐานสากลอย่างต่อเนื่อง โดยกรณีที่พบช่องโหว่ใหม่ สถาบันการเงินต้องเร่งดำเนินการให้มีแนวทางป้องกัน เพื่อปิดช่องโหว่ภายในกรอบเวลาที่เหมาะสม หรือดำเนินการให้แล้วเสร็จภายในระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนด

5.4 การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

กรณีที่สถาบันการเงินมีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ได้ ให้ยื่นขอผ่อนผันเป็นรายกรณีต่อธนาคารแห่งประเทศไทย พร้อมแสดงเหตุผลความจำเป็นและแผนการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธนาคารแห่งประเทศไทยจะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน โดยธนาคารแห่งประเทศไทยอาจกำหนดเงื่อนไขใด ๆ ให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

6. บทเฉพาะกาล

กรณีที่สถาบันการเงินมีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้อยู่ก่อนที่ประกาศฉบับนี้ใช้บังคับ และประสงค์จะขอผ่อนผันการปฏิบัติตามหลักเกณฑ์ดังกล่าว ให้สถาบันการเงินยื่นคำขอผ่อนผันตามหลักเกณฑ์ข้อ 5.4 ภายใน 7 วัน นับแต่วันที่ประกาศฉบับนี้มีผลใช้บังคับ โดยให้ถือว่าการปฏิบัติในระหว่างระยะเวลาการขอผ่อนผันและการพิจารณาผ่อนผันของ ธปท. ดังกล่าวไม่เป็นการฝ่าฝืนหลักเกณฑ์ของประกาศนี้

7. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป เว้นแต่กรณีตามข้อ 5.3.2 (3.3) ให้ใช้บังคับเมื่อพ้นกำหนดหกสิบวันนับแต่วันถัดจากประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ 31 มกราคม 2568

(นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6347, 0 2283 6346

คำถาม – คำตอบแนบท้ายประกาศ

เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงิน
บนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงิน

ลำดับ	คำถาม	คำตอบ
1	ขอทราบว่า ในกรณี สถาบันการเงินไม่ได้ให้บริการ Mobile Banking ผ่านแอปพลิเคชันของตนเอง แต่ให้บริการ Mobile Banking เป็นส่วนหนึ่งของแอปพลิเคชันของผู้ให้บริการอื่น (app-in-app) นั้น กรณีดังกล่าวเข้าข่ายต้องปฏิบัติตามประกาศฯ ฉบับนี้ด้วยหรือไม่	สถาบันการเงินที่ให้บริการ Mobile Banking ต้องดูแลให้บริการมีมาตรการควบคุมเป็นไปตามประกาศฯ ฉบับนี้ ไม่ว่าผู้ใช้บริการเข้าใช้ผ่านแอปพลิเคชันของสถาบันการเงินเอง หรือเข้าใช้งานผ่านแอปพลิเคชันของผู้ให้บริการอื่น
2	ขอทราบขอบเขตลิงก์ที่เข้าข่ายต้องงดเว้นแนบผ่านช่องทางข้อความสั้น (SMS) และช่องทางอีเมล	ขอบเขตการงดเว้นการแนบลิงก์ผ่านช่องทางข้อความสั้น (SMS) และช่องทางอีเมล ครอบคลุมลิงก์ทุกประเภท เช่น URL, ข้อความในลักษณะ URL ที่ไม่สามารถคลิกได้, รูปภาพที่มีข้อความในลักษณะ URL, ลิงก์ที่ฝังในรูปภาพ (clickable image links) ลิงก์ในลักษณะ QR code เป็นต้น
3	ขอให้ขยายความเรื่อง การส่ง SMS แนบลิงก์กรณีผู้ใช้บริการดำเนินการร้องขอเอง สถาบันการเงินสามารถแนบลิงก์ได้เป็นรายครั้ง	สถาบันการเงินสามารถแนบลิงก์ผ่านช่องทางข้อความสั้น (SMS) หรือช่องทางอีเมล ได้เฉพาะกรณีผู้ใช้บริการร้องขอเพื่อประโยชน์ในการใช้บริการในแต่ละครั้งเท่านั้น เช่น ขอข้อมูลการใช้บริการหรือผลิตภัณฑ์ ขอทราบข้อมูลการแก้ไขปัญหาการใช้งาน เป็นต้น รวมทั้ง สถาบันการเงินต้องสื่อสารให้ผู้ใช้บริการทราบอย่างชัดเจนว่า การแนบลิงก์ดังกล่าว ดำเนินการเฉพาะกรณีที่ร้องขอในครั้งนั้นเท่านั้น
4	ขอให้ขยายความการดำเนินการตามข้อกำหนดเรื่อง ให้มีกระบวนการรับมือและตอบสนองอย่างเหมาะสมและทันการณ์ต่อแอปพลิเคชันที่ปลอมแปลงหรือแอบอ้างเป็นแอปพลิเคชันของสถาบันการเงิน	สถาบันการเงินต้องกำหนดแนวทางและกระบวนการรับมือแอปพลิเคชันที่ปลอมแปลงหรือแอบอ้างเป็นแอปพลิเคชันของสถาบันการเงิน โดยอย่างน้อยครอบคลุม การกำหนดผู้รับผิดชอบ การกำหนดขั้นตอนการรับมือและแจ้ง take down แอปพลิเคชันที่ปลอมแปลงหรือแอบอ้าง

ลำดับ	คำถาม	คำตอบ
		เป็นสถาบันการเงิน การกำหนดระยะเวลาที่ต้องดำเนินการแล้วเสร็จในแต่ละขั้นตอน
5	ขอทราบตัวอย่างแพลตฟอร์มที่เป็นทางการของผู้ให้บริการดาวน์โหลดแอปพลิเคชัน (official app store)	ขอบเขตครอบคลุม ทั้งแพลตฟอร์มของผู้ให้บริการระบบปฏิบัติการ (OS) เช่น Google Play Store, Apple App Store, Huawei AppGallery เป็นต้น และแพลตฟอร์มของผู้ผลิตอุปกรณ์เคลื่อนที่ เช่น Samsung Galaxy Store เป็นต้น
6	กรณี สถาบันการเงินมีบริการ Mobile Banking มากกว่า 1 แอปพลิเคชัน สถาบันการเงินต้องจำกัดบัญชีผู้ใช้งานของทุกแอปพลิเคชันเพียง 1 บัญชีผู้ใช้งาน และจำกัดให้ใช้งานแอปพลิเคชันทั้งหมดบน 1 อุปกรณ์ หรือไม่	การจำกัดการใช้บริการ Mobile Banking ของผู้ใช้บริการเพียง 1 บัญชีผู้ใช้งาน และจำกัดการใช้บริการโดยให้ใช้งานบน 1 อุปกรณ์เคลื่อนที่ ให้ดำเนินการเป็นรายแอปพลิเคชัน
7	ขอบเขตบริการโอนเงินที่เข้าข่ายต้องยืนยันตัวตนผู้ใช้บริการเพิ่มเติมโดยใช้เทคโนโลยีเปรียบเทียบใบหน้า ครอบคลุมการโอนเงินลักษณะใดบ้าง	ขอบเขตครอบคลุม บริการโอนเงินทุกประเภท เช่น บริการโอนเงินภายในประเทศทั้งภายในธนาคารและต่างธนาคาร บริการโอนเงินธนาคารต่างประเทศ และบริการโอนเงินด้วย Thai QR ผ่าน PromptPay เป็นต้น
8	ขอทราบแนวทางการลดความเสี่ยงสำหรับผู้ใช้บริการคนพิการทางสายตา ซึ่งไม่สามารถใช้เทคโนโลยีเปรียบเทียบใบหน้าในการยืนยันตัวตน	กรณีคนพิการทางสายตาที่มีข้อจำกัดในการใช้เทคโนโลยีเปรียบเทียบใบหน้า สถาบันการเงินต้องมีกระบวนการระบุและพิสูจน์ตัวตนของผู้ใช้บริการดังกล่าว และมีแนวทางลดความเสี่ยง เช่น การจำกัดวงเงินการทำธุรกรรม การใช้วิธีการยืนยันตัวตนด้วยเทคโนโลยีอื่นที่มีความปลอดภัยตามมาตรฐานสากล เป็นต้น
9	สถาบันการเงินมีการกำหนดเพดานวงเงินสูงสุดต่อวันสำหรับกลุ่มผู้ใช้บริการที่มีความเสี่ยง เช่น กลุ่มผู้ใช้บริการที่อายุต่ำกว่า 15 ปี อย่างไรก็ดี หากผู้ใช้บริการขอยกเว้นการ	สถาบันการเงินต้องมีกระบวนการพิสูจน์ตัวตนผู้ใช้บริการ รวมทั้ง พิจารณาเหตุผลความจำเป็นในการขอยกเว้น ซึ่งสถาบันการเงินควรจัดทำเกณฑ์สำหรับการขอยกเว้นเพื่อให้การปฏิบัติงานมีมาตรฐานที่ชัดเจนและรัดกุม นอกจากนี้ สถาบัน

ลำดับ	คำถาม	คำตอบ
	กำหนดวงเงินดังกล่าว สถาบันการเงินต้องดำเนินการอย่างไร	การเงินต้องแจ้งให้ผู้ใช้บริการรับทราบถึงความเสี่ยงที่อาจได้รับหากเกิดเหตุการณ์ภัยทุจริตอย่างชัดเจน