



ธนาคารแห่งประเทศไทย

8 สิงหาคม 2568

เรียน ผู้จัดการ

สถาบันการเงินเฉพาะกิจทุกแห่ง

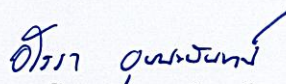
ที่ ธพท. 5054/2568 เรื่อง นำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงินเฉพาะกิจ

ธนาคารแห่งประเทศไทย (ธพท.) ขอนำส่งประกาศธนาคารแห่งประเทศไทย ที่ 17/2568 เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงินเฉพาะกิจ (ประกาศฯ) ซึ่งได้ประกาศลงในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 142 ตอนพิเศษ 267 ง วันที่ 7 สิงหาคม 2568 แล้ว และมีผลบังคับใช้เมื่อพ้นกำหนด 30 วัน นับแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

สาระสำคัญของการออกประกาศฯ เพื่อเป็นการยกระดับการให้บริการ Mobile Banking ให้มีมาตรฐานขั้นต่ำที่จำเป็นสำหรับการให้บริการทางการเงินและการชำระเงินบนแอปพลิเคชันของสถาบันการเงินเฉพาะกิจอย่างปลอดภัย โดยสถาบันการเงินเฉพาะกิจมีหน้าที่ต้องติดตามดูแล และปรับปรุงระบบงานและบริการ Mobile Banking ให้มีความมั่นคงปลอดภัยตามมาตรฐานสากล เท้าทันภัยคุกคามทางไซเบอร์และภัยทุกรูปแบบใหม่ที่มีเทคนิคซับซ้อนขึ้น ครอบคลุมทั้งในส่วนของระบบการให้บริการของสถาบันการเงินเฉพาะกิจ และความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ



(นางสาวโรร่า อุนนะนันท์)

ผู้อำนวยการอาวุโส ฝ่ายกำกับและตรวจสอบความเสี่ยง

ด้านเทคโนโลยีสารสนเทศ

ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย ประกาศธนาคารแห่งประเทศไทย ที่ 17/2568 เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงินเฉพาะกิจ

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

โทรศัพท์ 0 2283 6347 (สุรุต ทังสุฤติ), 0 2283 6364 (ชลวรรธ จิรเมธธร)

ไปรษณีย์อิเล็กทรอนิกส์ ITSupervision@bot.or.th

หมายเหตุ [X] ธพท. จัดประชุมชี้แจงในวันที่ 17 ธันวาคม 2567

[] ไม่มีการประชุมชี้แจง

วิสัยทัศน์ เป็นองค์กรที่มองไกล มีหลักการ และร่วมมือ เพื่อความเป็นอยู่ที่ดีอย่างยั่งยืนของไทย

www.bot.or.th



ประกาศธนาคารแห่งประเทศไทย

ที่ 17 /2568

เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่
สำหรับสถาบันการเงินเฉพาะกิจ

1. เหตุผลในการออกประกาศ

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology : IT) มีบทบาทสำคัญสำหรับการดำเนินธุรกิจของสถาบันการเงินเฉพาะกิจ โดยเฉพาะการให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันของสถาบันการเงินเฉพาะกิจแก่ผู้ใช้บริการที่เป็นบุคคลธรรมดาบนอุปกรณ์เคลื่อนที่ (บริการ Mobile Banking) ที่มีการใช้งานเพิ่มขึ้นอย่างรวดเร็วและยังคงขยายตัวอย่างต่อเนื่อง ขณะเดียวกัน การให้บริการ Mobile Banking ก็นำมาซึ่งความเสี่ยงจากภัยคุกคามทางไซเบอร์ (cyber threat) และภัยทุจริตทางการเงิน (fraud) ที่มีการปรับเปลี่ยนรูปแบบและใช้เทคนิควิธีการที่ซับซ้อนมากขึ้น อันอาจสร้างความเสียหายต่อผู้ใช้บริการในวงกว้าง ส่งผลกระทบต่อความน่าเชื่อถือของระบบสถาบันการเงินและระบบการชำระเงินของประเทศ

ธนาคารแห่งประเทศไทยตระหนักถึงความสำคัญในการป้องกันภัยทุจริตดังกล่าว จึงได้ออกประกาศหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่เพื่อยกระดับการให้บริการ Mobile Banking ให้มีมาตรฐานขั้นต่ำที่จำเป็นสำหรับการให้บริการทางการเงินและการชำระเงินบนแอปพลิเคชันของสถาบันการเงินเฉพาะกิจให้เป็นไปอย่างปลอดภัยเท่าทันความเสี่ยงจากภัยคุกคามทางไซเบอร์และภัยทุจริตทางการเงินที่มีการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (Unauthorized Payment Fraud)

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 120/1 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 และที่แก้ไขเพิ่มเติม ธนาคารแห่งประเทศไทยโดยความเห็นชอบของรัฐมนตรีว่าการกระทรวงการคลังออกหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงินเฉพาะกิจ ให้สถาบันการเงินเฉพาะกิจถือปฏิบัติตามที่กำหนดในประกาศนี้

3. แนวนโยบายที่ยกเลิก

3.1 แนวนโยบาย เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ของสถาบันการเงินเฉพาะกิจ ตามหนังสือเวียนธนาคารแห่งประเทศไทย ที่ ฝนส2. 271/2564 ลงวันที่ 12 เมษายน 2564

3.2 ข้อ 1.2 ข้อ 1.4 และข้อ 1.6 ในเอกสารแนบ 2 ของแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ตามหนังสือเวียนธนาคารแห่งประเทศไทย ที่ ธปท.ผนช.(02) ว. 224/2566 ลงวันที่ 29 มีนาคม 2566

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับสถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

5. เนื้อหา

5.1 คำจำกัดความ

ในประกาศฉบับนี้

“อุปกรณ์เคลื่อนที่” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์แบบพกพาซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่น เพื่อรับหรือส่งข้อมูลทางการเงิน การชำระเงิน หรือคำสั่งการชำระเงินผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง

“สถาบันการเงินเฉพาะกิจ” หมายความว่า สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“ผู้ใช้บริการ” หมายความว่า บุคคลธรรมดาที่ใช้บริการทางการเงินและการชำระเงินผ่านบริการ Mobile Banking บนอุปกรณ์เคลื่อนที่

“บริการ Mobile Banking” หมายความว่า การให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันของสถาบันการเงินเฉพาะกิจที่มีการให้บริการแก่ผู้ใช้บริการบนอุปกรณ์เคลื่อนที่ซึ่งให้บริการถอนเงิน โอนเงิน หรือการชำระค่าสินค้าและบริการ อย่างใดอย่างหนึ่ง

“การสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (Unauthorized Payment Fraud)” หมายถึง ภัยทุจริตทางการเงินที่เกิดขึ้นจากการที่ผู้อื่นสวมรอยทำธุรกรรมแทนผู้ใช้บริการโดยทุจริตโดยที่ผู้ใช้บริการไม่ได้ให้ความยินยอม เช่น กรณีผู้ไม่ประสงค์ดีติดตั้ง malware บนอุปกรณ์เคลื่อนที่

ของผู้ใช้บริการ ทำให้สามารถเข้าถึงหรือควบคุมอุปกรณ์เคลื่อนที่และแอปพลิเคชัน และสวมรอยทำธุรกรรมผ่านบัญชีของผู้ใช้บริการโดยไม่ได้รับอนุญาต

5.2 หลักการ

สถาบันการเงินเฉพาะกิจที่ให้บริการ Mobile Banking บนอุปกรณ์เคลื่อนที่มีหน้าที่ต้องติดตามดูแลและปรับปรุงระบบงานและบริการ Mobile Banking ให้มีความมั่นคงปลอดภัยตามมาตรฐานสากล เท่าทันภัยคุกคามทางไซเบอร์และภัยทุกรูปแบบใหม่ที่มีเทคนิคซับซ้อนขึ้นครอบคลุมทั้งในส่วนของการให้บริการของสถาบันการเงินเฉพาะกิจ และความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ

5.3 หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่

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

5.3.1 การป้องกันการสวมรอยทำธุรกรรมแทนผู้ให้บริการ

สถาบันการเงินเฉพาะกิจต้องมีการป้องกันการสวมรอยทำธุรกรรมแทนผู้ให้บริการ โดยอย่างน้อยต้องดำเนินการ ดังต่อไปนี้

(1) งดเว้นการแนบลิงก์ผ่านช่องทางข้อความสั้น (SMS) และช่องทางอีเมล แต่สำหรับกรณีช่องทางสื่อสังคมออนไลน์ (social media) ให้สถาบันการเงินเฉพาะกิจดแนบลิงก์เฉพาะที่มีการขอข้อมูลในการยืนยันตัวตนหรือข้อมูลส่วนบุคคล เช่น ชื่อผู้ใช้งาน รหัสผ่าน รหัสใช้ครั้งเดียว (one time password - OTP) รหัส PIN หมายเลขบัตรประชาชน วันเดือนปีเกิด เพื่อป้องกันการสวมรอยเป็นสถาบันการเงินเฉพาะกิจ การขอให้เปิดเผยข้อมูลสำคัญ (social engineering) หรือการถูกติดตั้ง mobile malware

อย่างไรก็ดี สถาบันการเงินเฉพาะกิจสามารถแนบลิงก์ผ่านทั้ง 3 ช่องทางดังกล่าวได้ หากผู้ให้บริการดำเนินการร้องขอเอง โดยสถาบันการเงินเฉพาะกิจสามารถแนบลิงก์ได้เป็นรายครั้ง พร้อมทั้งต้องมีการสื่อสารย้ำให้ผู้บริการทราบว่าการส่งลิงก์ดังกล่าวเป็นกรณีเฉพาะตามคำร้องขอของผู้บริการเป็นรายครั้งเท่านั้น

(2) มีกระบวนการติดตามและรับมืออย่างทันการณืต่อแอปพลิเคชันที่ปลอมแปลงหรือแอบอ้างเป็นแอปพลิเคชันของสถาบันการเงินเฉพาะกิจที่ให้บริการ Mobile Banking ในแพลตฟอร์มที่เป็นทางการของผู้ให้บริการดาวน์โหลดแอปพลิเคชัน (official app store) เช่น Google Play Store Apple App Store รวมทั้งมีกระบวนการรับมือและตอบสนองอย่างเหมาะสมและทันการณืสำหรับแอปพลิเคชันปลอมแปลงที่อยู่นอกแพลตฟอร์มดังกล่าว เพื่อลดความเสี่ยงที่ผู้ให้บริการจะหลงเชื่อและเปิดเผยข้อมูลสำคัญ ถูกติดตั้ง malware หรือถูกติดตั้งแอปพลิเคชันปลอม

(3) จำกัดการใช้บริการ Mobile Banking ของผู้ให้บริการไว้เพียง 1 บัญชีผู้ใช้งานต่อ 1 บริการ Mobile Banking ของแต่ละสถาบันการเงินเฉพาะกิจ และจำกัดการใช้บริการดังกล่าว โดยให้ใช้งานบน 1 อุปกรณ์เคลื่อนที่ของผู้ให้บริการเท่านั้น

(4) ต้องจัดให้มีกระบวนการยืนยันตัวตนผู้ให้บริการเพิ่มเติมในขั้นตอนการทำธุรกรรมผ่านบริการ Mobile Banking บนอุปกรณ์เคลื่อนที่ โดยใช้เทคโนโลยีเปรียบเทียบใบหน้า (face comparison) ร่วมกับการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) ที่สามารถป้องกันการใช้รูปภาพ วิดีโอ หรือการปลอมแปลงชีวมิติในรูปแบบต่าง ๆ ได้ เช่น การใช้เทคโนโลยี liveness detection เพื่อให้มั่นใจว่าผู้ให้บริการเป็นผู้ทำธุรกรรมด้วยตนเอง ซึ่งต้องจัดให้มีกระบวนการยืนยันตัวตนผู้ให้บริการเพิ่มเติมดังกล่าวอย่างน้อยในกรณีดังต่อไปนี้

(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 กรณีที่ผู้ให้บริการมีข้อจำกัดในการใช้เทคโนโลยีเปรียบเทียบใบหน้า (face comparison) เช่น เป็นคนพิการทางสายตา สถาบันการเงินเฉพาะกิจอาจพิจารณางดเว้นการยืนยันตัวตนเพิ่มเติมตามที่กำหนดข้างต้นได้ โดยต้องมีแนวทางลดความเสี่ยงทดแทน หรือกรณีการทำธุรกรรมที่มีความเสี่ยงต่ำ เช่น การทำธุรกรรมโอนเงินระหว่างบัญชีตนเอง การทำธุรกรรมโอนเงินประจำอัตโนมัติ (automatic recurring transfer) ที่ได้ยืนยันตัวตนไปแล้วในครั้งแรก สถาบันการเงินเฉพาะกิจอาจพิจารณางดเว้นการยืนยันตัวตนเพิ่มเติมตามที่กำหนดข้างต้นได้

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

ทั้งนี้ สถาบันการเงินเฉพาะกิจสามารถใช้แนวทางหรือข้อกำหนดที่ได้จัดทำร่วมกัน (industry standard) มาใช้ประกอบการจัดระดับความเสี่ยง หรือกำหนดเพดานวงเงินสูงสุดของกลุ่มผู้ใช้บริการได้ และในกรณีที่ผู้ใช้บริการขอยกเว้นการกำหนดวงเงินตามกลุ่มความเสี่ยงที่กำหนดไว้ สถาบันการเงินเฉพาะกิจต้องมีกระบวนการพิจารณาการขอยกเว้นที่ชัดเจนและรัดกุมด้วย

5.3.2 การรักษาความมั่นคงปลอดภัยของบริการ Mobile Banking

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

(1) การรักษาความมั่นคงปลอดภัยของข้อมูล

สถาบันการเงินเฉพาะกิจต้องรักษาความลับและความปลอดภัยของข้อมูลสำคัญของผู้ใช้บริการอย่างรัดกุม เพื่อป้องกันข้อมูลสำคัญของผู้ใช้บริการรั่วไหล หรือถูกเปลี่ยนแปลงแก้ไข ทั้งขณะจัดเก็บ แสดงผล และรับ-ส่งข้อมูลระหว่างอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ และระบบงานของสถาบันการเงินเฉพาะกิจ โดยต้องดำเนินการอย่างน้อย ดังนี้

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

(1.2) แอปพลิเคชันของสถาบันการเงินเฉพาะกิจต้องแสดงผลข้อมูลสำคัญ (sensitive information) ของผู้ใช้บริการเท่าที่จำเป็นและเป็นไปอย่างรัดกุม โดยอย่างน้อยต้องปิดบังการแสดงผลข้อมูลที่สลับผ่าน และปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (application blurring)

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

(2) การรักษาความมั่นคงปลอดภัยของแอปพลิเคชัน

สถาบันการเงินเฉพาะกิจต้องติดตามดูแลและปรับปรุงแอปพลิเคชันให้มีความมั่นคงปลอดภัยตามมาตรฐานสากลและเท่าทันภัยคุกคามรูปแบบใหม่อยู่เสมอ โดยต้องดำเนินการอย่างน้อย ดังนี้

(2.1) แอปพลิเคชันของสถาบันการเงินเฉพาะกิจต้องขอสิทธิเข้าถึงทรัพยากรหรือบริการบนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ (application permission) เท่าที่จำเป็นและมีการทบทวนการขอสิทธิดังกล่าวทุกครั้งที่มีการเปลี่ยนแปลงแอปพลิเคชันอย่างมีนัยสำคัญ เพื่อป้องกันการละเมิดสิทธิความเป็นส่วนตัวของผู้ใช้บริการ รวมถึงเป็นช่องโหว่ที่อาจถูกใช้โดยผู้อื่นที่กระทำการโดยทุจริต

(2.2) ไม่ให้บริการบนแอปพลิเคชันเวอร์ชันเก่าที่อาจมีช่องโหว่ และอาจทำให้เกิดความเสี่ยงในการสวมรอยทำธุรกรรมแทนผู้ให้บริการ

(2.3) ตรวจสอบการเปลี่ยนแปลงแก้ไขแอปพลิเคชันทุกครั้งในทันทีที่ผู้ให้บริการเข้าใช้งาน (anti-tampering) และไม่อนุญาตให้ผู้ให้บริการใช้งานแอปพลิเคชันที่ถูกเปลี่ยนแปลงแก้ไข เพื่อป้องกันไม่ให้ข้อมูลผู้ให้บริการรั่วไหลหรือเกิดความเสียหายจากแอปพลิเคชันที่มีการดัดแปลงแก้ไข เช่น การฝัง malicious code

(2.4) จัดการการเชื่อมต่อระหว่างคอมพิวเตอร์ (session) ให้ปลอดภัย เพื่อป้องกันการสวมรอยเข้าใช้งานโดยไม่ได้รับอนุญาต (session hijacking)

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

(3) การรักษาความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่

สถาบันการเงินเฉพาะกิจต้องให้บริการ Mobile Banking ในสภาพแวดล้อมของอุปกรณ์เคลื่อนที่ที่ปลอดภัย เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีกระทำการทุจริตโดยอาศัยช่องโหว่ของระบบปฏิบัติการเข้าถึง Mobile Banking และบัญชีของผู้ใช้บริการ โดยต้องดำเนินการอย่างน้อย ดังนี้

(3.1) ไม่อนุญาตให้แอปพลิเคชันของสถาบันการเงินเฉพาะกิจใช้งานบนอุปกรณ์เคลื่อนที่ที่ตรวจพบว่าการเปิดสิทธิให้เข้าถึงระบบปฏิบัติการ (rooted/jailbroken)

(3.2) ไม่อนุญาตให้แอปพลิเคชันของสถาบันการเงินเฉพาะกิจทำงานบนอุปกรณ์เคลื่อนที่ในขณะที่มีแอปพลิเคชันอื่นกำลังทำงานและมีพฤติกรรมการทำงานที่เสี่ยงจะก่อให้เกิดการสวมรอยทำธุรกรรมแทนผู้ให้บริการ เช่น แอปพลิเคชันที่ขอสิทธิช่วยเหลือคนพิการ (accessibility services) โดยไม่จำเป็น แอปพลิเคชันที่สามารถควบคุมอุปกรณ์เคลื่อนที่จากระยะไกลได้ (remote control) แอปพลิเคชันที่มีการปิดบังหรือขโมยข้อมูลที่แสดงบนหน้าจอของผู้ใช้งาน เพื่อลดความเสี่ยงที่

แอปพลิเคชันของสถาบันการเงินเฉพาะกิจจะถูกควบคุมหรือเข้าถึงโดย malware ที่มีการติดตั้งบนอุปกรณ์เคลื่อนที่

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

กรณีสถาบันการเงินเฉพาะกิจมีการให้บริการบนอุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการที่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ หรือการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ สถาบันการเงินเฉพาะกิจต้องจัดให้มีแนวทางการควบคุมความเสี่ยงเพิ่มเติม โดยการแจ้งเตือนถึงความเสี่ยงจากกรณีดังกล่าว รวมทั้งจำกัดวงเงินการทำธุรกรรมของกลุ่มผู้ใช้บริการดังกล่าวให้ทำธุรกรรมโอนเงินได้ไม่เกินวันละ 5,000 บาท

ทั้งนี้ สถาบันการเงินเฉพาะกิจต้องติดตามและปรับปรุงการรักษาความมั่นคงปลอดภัยของการให้บริการ Mobile Banking ให้เท่าทันภัยคุกคามทางไซเบอร์และภัยทุจริตรูปแบบใหม่ เป็นไปตามมาตรฐานสากลอย่างต่อเนื่อง โดยกรณีที่เกิดช่องโหว่ใหม่ สถาบันการเงินเฉพาะกิจต้องเร่งดำเนินการให้มีแนวทางป้องกัน เพื่อปิดช่องโหว่ภายในกรอบเวลาที่เหมาะสม หรือดำเนินการให้แล้วเสร็จภายในระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนด

5.4 การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

กรณีที่สถาบันการเงินเฉพาะกิจมีเหตุจำเป็นหรือเหตุการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ได้ ให้ยื่นขอผ่อนผันเป็นรายการณ์ต่อธนาคารแห่งประเทศไทย พร้อมแสดงเหตุผลความจำเป็นและแผนการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ ธนาคารแห่งประเทศไทยจะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการ นับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน โดยธนาคารแห่งประเทศไทยอาจกำหนดเงื่อนไขใด ๆ ให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

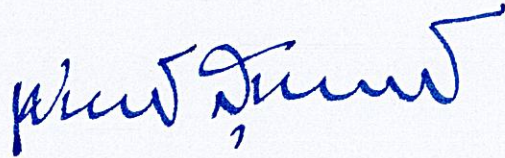
6. บทเฉพาะกาล

กรณีที่สถาบันการเงินเฉพาะกิจมีเหตุจำเป็นหรือเหตุการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้อยู่ก่อนที่ประกาศฉบับนี้ใช้บังคับ และประสงค์จะขอผ่อนผันการปฏิบัติตามหลักเกณฑ์ดังกล่าว ให้สถาบันการเงินเฉพาะกิจยื่นคำขอผ่อนผันตามหลักเกณฑ์ข้อ 5.4 ภายใน 7 วัน นับแต่วันที่ประกาศฉบับนี้มีผลใช้บังคับ โดยให้ถือว่าการปฏิบัติในระหว่างระยะเวลาการขอผ่อนผันและการพิจารณาผ่อนผันของธนาคารแห่งประเทศไทยดังกล่าวไม่เป็นการฝ่าฝืนหลักเกณฑ์ของประกาศนี้

7. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันถัดจากวันประกาศใน
ราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ 25 กรกฎาคม 2568



(นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ)

ผู้ว่าการ

ธนาคารแห่งประเทศไทย

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6347, 0 2283 6346

คำถาม – คำตอบแนบท้ายประกาศ

เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงิน
บนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงินเฉพาะกิจ

ลำดับ	คำถาม	คำตอบ
1	ขอทราบว่า ในกรณี สถาบันการเงินเฉพาะกิจ ไม่ได้ให้บริการ Mobile Banking ผ่านแอปพลิเคชันของตนเอง แต่ให้บริการ Mobile Banking เป็นส่วนหนึ่งของแอปพลิเคชันของผู้ให้บริการอื่น (app-in-app) นั้น กรณีดังกล่าวเข้าข่ายต้องปฏิบัติตามประกาศฉบับนี้ด้วยหรือไม่	สถาบันการเงินเฉพาะกิจที่ให้บริการ Mobile Banking ต้องดูแลให้บริการมีมาตรการควบคุมเป็นไปตามประกาศฯ ฉบับนี้ ไม่ว่าผู้ให้บริการเข้าใช้ผ่านแอปพลิเคชันของสถาบันการเงินเฉพาะกิจเอง หรือเข้าใช้งานผ่านแอปพลิเคชันของผู้ให้บริการอื่น
2	ขอทราบขอบเขตลิงก์ที่เข้าข่ายต้องดเว้นแนบผ่านช่องทางข้อความสั้น (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 สถาบันการเงินเฉพาะกิจสามารถแนบลิงก์ได้เป็นรายครั้ง	สถาบันการเงินเฉพาะกิจสามารถแนบลิงก์ผ่านช่องทางข้อความสั้น (SMS) หรือช่องทางอีเมล ได้เฉพาะกรณีผู้ใช้บริการร้องขอเพื่อประโยชน์ในการใช้บริการในแต่ละครั้งเท่านั้น เช่น ขอข้อมูลการใช้บริการหรือผลิตภัณฑ์ ขอทราบข้อมูลการแก้ไขปัญหาการใช้งาน เป็นต้น รวมทั้ง สถาบันการเงินเฉพาะกิจต้องสื่อสารให้ผู้ใช้บริการทราบอย่างชัดเจนว่า การแนบลิงก์ดังกล่าว ดำเนินการเฉพาะกรณีที่ร้องขอในครั้งนั้นเท่านั้น
4	ขอให้ขยายความการดำเนินการตามข้อกำหนดเรื่อง ให้มีกระบวนการรับมือและตอบสนองอย่างเหมาะสมและทันการณ์ต่อแอปพลิเคชันที่ปลอมแปลงหรือแอบอ้างเป็นแอปพลิเคชันของสถาบันการเงินเฉพาะกิจ	สถาบันการเงินเฉพาะกิจต้องกำหนดแนวทางและกระบวนการรับมือแอปพลิเคชันที่ปลอมแปลงหรือแอบอ้างเป็นแอปพลิเคชันของสถาบันการเงินเฉพาะกิจ โดยอย่างน้อยครอบคลุม การกำหนดผู้รับผิดชอบ การกำหนดขั้นตอนการรับมือและแจ้ง take down แอปพลิเคชันที่ปลอมแปลงหรือแอบอ้างเป็นสถาบันการเงินเฉพาะกิจ การกำหนดระยะเวลาที่ต้องดำเนินการแล้วเสร็จในแต่ละขั้นตอน

ลำดับ	คำถาม	คำตอบ
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 สถาบันการเงินเฉพาะกิจมีบริการ Mobile Banking มากกว่า 1 แอปพลิเคชัน สถาบันการเงินเฉพาะกิจต้องจำกัดบัญชีผู้ใช้งานของทุกแอปพลิเคชันเพียง 1 บัญชีผู้ใช้งาน และจำกัดให้ใช้งานแอปพลิเคชันทั้งหมดบน 1 อุปกรณ์ หรือไม่	การจำกัดการใช้บริการ Mobile Banking ของผู้ให้บริการเพียง 1 บัญชีผู้ใช้งาน และจำกัดการใช้บริการโดยให้ใช้งานบน 1 อุปกรณ์เคลื่อนที่ ให้ดำเนินการเป็นรายแอปพลิเคชัน
7	ขอบเขตบริการโอนเงินที่เข้าข่ายต้องยืนยันตัวตนผู้ให้บริการเพิ่มเติมโดยใช้เทคโนโลยีเปรียบเทียบกับหน้า ครอบคลุมการโอนเงินลักษณะใดบ้าง	ขอบเขตครอบคลุม บริการโอนเงินทุกประเภท เช่น บริการโอนเงินภายในประเทศทั้งภายในธนาคารและต่างธนาคาร บริการโอนเงินธนาคารต่างประเทศ และบริการโอนเงินด้วย Thai QR ผ่าน PromptPay เป็นต้น
8	ขอทราบแนวทางการลดความเสี่ยงสำหรับผู้ให้บริการคนพิการทางสายตา ซึ่งไม่สามารถใช้เทคโนโลยีเปรียบเทียบกับหน้าในการยืนยันตัวตน	กรณีคนพิการทางสายตาที่มีข้อจำกัดในการใช้เทคโนโลยีเปรียบเทียบกับหน้า สถาบันการเงินเฉพาะกิจต้องมีกระบวนการระบุและพิสูจน์ตัวตนของผู้ใช้บริการดังกล่าว และมีแนวทางลดความเสี่ยง เช่น การจำกัดวงเงินการทำธุรกรรม การใช้วิธีการยืนยันตัวตนด้วยเทคโนโลยีอื่นที่มีความปลอดภัยตามมาตรฐานสากล เป็นต้น
9	กรณีสถาบันการเงินเฉพาะกิจให้บริการลูกค้าชาวต่างชาติ ลูกค้ากลุ่มดังกล่าวต้องมีการยืนยันตัวตนเพิ่มเติมโดยใช้เทคโนโลยีเปรียบเทียบกับหน้าเมื่อทำธุรกรรมที่เข้าข่ายที่กำหนดในประกาศฯ ด้วยหรือไม่	สำหรับลูกค้าชาวต่างชาติ สถาบันการเงินเฉพาะกิจต้องจัดให้มีการยืนยันตัวตนเพิ่มเติมโดยใช้เทคโนโลยีเปรียบเทียบกับหน้าเมื่อทำธุรกรรมที่เข้าข่ายตามที่กำหนดในประกาศฯ เช่นเดียวกับลูกค้าคนไทย
10	สถาบันการเงินเฉพาะกิจมีการกำหนดเพดานวงเงินสูงสุดต่อวันสำหรับกลุ่มผู้ให้บริการที่มีความเสี่ยง เช่น กลุ่มผู้ให้บริการที่อายุต่ำกว่า 15 ปี อย่างไรก็ดี หากผู้ให้บริการขอยกเว้นการกำหนดวงเงินดังกล่าว สถาบันการเงินเฉพาะกิจต้องดำเนินการอย่างไร	สถาบันการเงินเฉพาะกิจต้องมีกระบวนการพิสูจน์ตัวตนผู้ให้บริการ รวมทั้ง พิจารณาเหตุผลความจำเป็นในการขอยกเว้น ซึ่งสถาบันการเงินเฉพาะกิจควรจัดทำเกณฑ์สำหรับการขอยกเว้นเพื่อให้การปฏิบัติงานมีมาตรฐานที่ชัดเจนและรัดกุม นอกจากนี้ สถาบันการเงินเฉพาะกิจต้องแจ้งให้

ลำดับ	คำถาม	คำตอบ
		ผู้ใช้บริการรับทราบถึงความเสี่ยงที่อาจได้รับหากเกิดเหตุการณ์ภัยทุจริตอย่างชัดเจน