ธนาคารแห่งประเทศไทย

8 สิงหาคม 2568

เรียน ผู้จัดการ

ธนาคารพาณิชย์ทุกแห่ง

สถาบันการเงินเฉพาะกิจทุกแห่ง

ที่ ธปท.ว. 5044 /2568 เรื่อง นำส่งประกาศธนาคารแห่งประเทศไทยว่าด้วยมาตรฐานและมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีสำหรับสถาบันการเงิน

ธนาคารแห่งประเทศไทยขอนำส่งประกาศธนาคารแห่งประเทศไทย ที่ 19/2568 เรื่อง มาตรฐานและมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีสำหรับสถาบันการเงิน ลงวันที่ 25 กรกฎาคม 2568 ซึ่งได้ประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 142 ตอนพิเศษ 267 ง ลงวันที่ 7 สิงหาคม 2568 และมีผลบังคับใช้ตั้งแต่วันที่ 8 สิงหาคม 2568 เป็นต้นไป

สาระสำคัญของการออกประกาศในครั้งนี้มีวัตถุประสงค์เพื่อเป็นการกำหนดมาตรฐานและมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีสำหรับธนาคารพาณิชย์และสถาบันการเงินเฉพาะกิจตามอำนาจหน้าที่ที่กำหนดในพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และที่แก้ไขเพิ่มเติม

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นางสาวดารณี แซ่จู)
ผู้ช่วยผู้ว่าการ สายกำกับระบบการชำระเงิน
และคุ้มครองผู้ใช้บริการทางการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย ประกาศธนาคารแห่งประเทศไทยที่ 19/2568 เรื่อง มาตรฐานและมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีสำหรับสถาบันการเงิน

งานจัดการภัยทุจริตทางการเงิน
โทรศัพท์ 0 2283 6168, 0 2283 6176
ไปรษณีย์อิเล็กทรอนิกส์ antifraud-policy@bot.or.th

ประกาศธนาคารแห่งประเทศไทย

ที่ ๑๙ / 2568

เรื่อง มาตรฐานและมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยี
สำหรับสถาบันการเงิน

---

1. เหตุผลในการออกประกาศ

สืบเนื่องจากอาชญากรรมทางเทคโนโลยีส่งผลให้ประชาชนจำนวนมากได้รับความเดือดร้อน ต้องสูญเสียเงินให้กับมิจฉาชีพเป็นมูลค่าสูงมาก ภาครัฐจึงได้มีการตราพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 เพื่อคุ้มครองประชาชนที่ถูกหลอกลวงผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์จนสูญเสียไปซึ่งทรัพย์สิน และต่อมาได้มีการปรับปรุงพระราชกำหนดดังกล่าว โดยมีการเพิ่มเติมมาตรการในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้ครอบคลุมรูปแบบและวิธีการที่หลากหลายมากยิ่งขึ้นในการหลอกลวงประชาชนของมิจฉาชีพ รวมทั้งกำหนดให้สถาบันการเงิน ผู้ประกอบธุรกิจ ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น ผู้ให้บริการอื่นที่เกี่ยวข้อง หรือผู้ให้บริการสื่อสังคมออนไลน์ มีส่วนร่วมรับผิดชอบในความเสียหายที่เกิดจากอาชญากรรมทางเทคโนโลยีให้แก่ผู้เสียหายตามสัดส่วนเท่าที่ผู้ประกอบการดังกล่าวแต่ละรายมีส่วนเกี่ยวข้องกับสาเหตุที่ทำให้เกิดความเสียหาย เว้นแต่บุคคลดังกล่าวจะพิสูจน์ได้ว่าได้ปฏิบัติตามมาตรฐานหรือมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีที่กำหนดโดยหน่วยงานกำกับดูแลที่เกี่ยวข้องแล้ว ทั้งนี้ เพื่อเป็นการผลักดันให้สถาบันการเงิน ผู้ประกอบธุรกิจ ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น ผู้ให้บริการอื่นที่เกี่ยวข้อง หรือผู้ให้บริการสื่อสังคมออนไลน์ ต้องยกระดับมาตรฐานหรือมาตรการป้องกันอาชญากรรมทางเทคโนโลยี พร้อมทั้งดูแลรับผิดชอบการให้บริการทางเทคโนโลยีแก่ประชาชนผู้ใช้บริการตามสมควรแก่ประเภทของแต่ละธุรกิจ พระราชกำหนดดังกล่าวจึงกำหนดให้หน่วยงานกำกับดูแลกำหนดมาตรฐานและมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยี

ธนาคารแห่งประเทศไทยจึงกำหนดหลักเกณฑ์เพื่อเป็นมาตรฐานและมาตรการในการป้องกันอาชญากรรมทางเทคโนโลยีสำหรับสถาบันการเงินที่กำหนดตามพระราชกำหนดดังกล่าว ได้แก่ ธนาคารพาณิชย์และสถาบันการเงินของรัฐที่มีกฎหมายเฉพาะจัดตั้งขึ้นตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามมาตรา 4/1 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และที่แก้ไขเพิ่มเติม

3. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับสถาบันการเงินตามกฎหมายว่าด้วยมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

4. เนื้อหา

4.1 คำจำกัดความ

ในประกาศฉบับนี้

“พระราชกำหนด” หมายความว่า พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และที่แก้ไขเพิ่มเติม

“สถาบันการเงิน” หมายความว่า ธนาคารพาณิชย์และสถาบันการเงินของรัฐที่มีกฎหมายเฉพาะจัดตั้งขึ้น ทั้งนี้ ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“ลูกค้า” หมายความว่า บุคคลธรรมดา นิติบุคคล หรือบุคคลที่มีการตกลงกันทางกฎหมาย ซึ่งสร้างความสัมพันธ์ทางธุรกิจหรือทำธุรกรรมกับสถาบันการเงิน

“บริการ Mobile Banking” หมายความว่า การให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันของสถาบันการเงินที่มีการให้บริการแก่ผู้ใช้บริการบนอุปกรณ์เคลื่อนที่ซึ่งให้บริการถอนเงิน โอนเงิน หรือการชำระค่าสินค้าและบริการ อย่างใดอย่างหนึ่ง

“ผู้ใช้บริการ” หมายความว่า บุคคลธรรมดาที่ใช้บริการทางการเงินและการชำระเงินผ่านบริการ Mobile Banking บนอุปกรณ์เคลื่อนที่

“ระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล” หมายความว่า ระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา 4 วรรค 1 แห่งพระราชกำหนด

“ผู้ประกอบธุรกิจ” หมายความว่า ผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงินและผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลตามกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล

“บัญชีม้า” หมายความว่า บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ ซึ่งถูกนำมาใช้หรืออาจถูกนำมาใช้เป็นเครื่องมือในการรับเงินและถ่ายโอนเงินที่ได้มาจากอาชญากรรมทางเทคโนโลยี

“บัญชีม้าดำ” หมายความว่า บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลที่มีรายชื่อเป็นบุคคลที่มีความเสี่ยงสูงซึ่งควรได้รับการเฝ้าระวังอย่างใกล้ชิดตามกฎกระทรวงการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า พ.ศ. 2563 กรณีบัญชีม้า (รหัส HR-03-01 รหัส HR-03-02) ทั้งนี้ ให้หมายถึงเฉพาะรายชื่อบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามกฎหมายว่าด้วยมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

“บัญชีม้าเทาเข้ม” หมายความว่า บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลที่มีรายชื่อเป็นม้าเทาเข้มในระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล

“บัญชีม้าเทาอ่อน” หมายความว่า บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลที่มีรายชื่อเป็นม้าเทาอ่อนในระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล

“ช่องทางดิจิทัล” หมายความว่า การให้บริการทางอินเทอร์เน็ต (Internet Banking) และอุปกรณ์เคลื่อนที่ (Mobile Banking)

“สาขา” หมายความว่า การให้บริการที่มีสถานที่ทำการที่แน่นอนและให้บริการโดยพนักงานของสถาบันการเงิน

4.2 หลักเกณฑ์

สถาบันการเงินต้องถือปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ เพื่อป้องกันอาชญากรรมทางเทคโนโลยี ซึ่งจะช่วยลดความเสียหายที่จะเกิดขึ้นกับประชาชน และรักษาความเชื่อมั่นในระบบสถาบันการเงินและระบบการชำระเงินของประเทศ โดยในกรณีที่ความเสียหายดังกล่าวเกี่ยวข้องโดยตรงกับการที่สถาบันการเงินไม่ปฏิบัติตามหลักเกณฑ์ซึ่งเป็นมาตรฐานหรือมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีตามประกาศนี้ สถาบันการเงินต้องมีส่วนรับผิดชอบในความเสียหายที่เกิดจากอาชญากรรมทางเทคโนโลยีตามสัดส่วนแห่งพฤติการณ์ของสถาบันการเงิน ลูกค้า ผู้ประกอบธุรกิจ รวมทั้งบุคคลอื่น ตามที่แต่ละบุคคลจะมีส่วนเกี่ยวข้องกับสาเหตุที่ทำให้เกิดความเสียหาย

4.2.1 การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (unauthorized payment fraud)

สถาบันการเงินต้องมีการป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการและรักษาความมั่นคงปลอดภัยแอปพลิเคชันที่ให้บริการ Mobile Banking ที่มีการให้บริการแก่ลูกค้าที่เป็นบุคคลธรรมดา เพื่อป้องกันความเสี่ยงจากอาชญากรรมทางเทคโนโลยี ดังนี้

(1) ไม่แนบลิงก์ที่เป็นเหตุให้เกิดความเสียหายแก่ผู้ใช้บริการผ่านช่องทางข้อความสั้น (SMS) ช่องทางอีเมล และช่องทางสื่อสังคมออนไลน์ (social media)

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

(3) จัดให้มีกระบวนการยืนยันตัวตนผู้ใช้บริการเพิ่มเติม โดยใช้เทคโนโลยีเปรียบเทียบใบหน้า (face comparison) ร่วมกับการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) ที่สามารถป้องกันการใช้รูปภาพ วิดีโอ หรือการปลอมแปลงชีวมิติในรูปแบบต่าง ๆ ได้

เช่น การใช้เทคโนโลยี liveness detection เพื่อให้มั่นใจว่าผู้ใช้บริการเป็นผู้ทำธุรกรรมด้วยตนเอง ในกรณีที่มีการทำธุรกรรมผ่านบริการ Mobile Banking ในขั้นตอนดังต่อไปนี้

(3.1) การทำธุรกรรมโอนเงินในครั้งที่มีมูลค่าตั้งแต่ 50,000 บาทขึ้นไป หรือ

(3.2) การทำธุรกรรมโอนเงินมูลค่ารวมกันครบทุก 200,000 บาท ในรอบระยะเวลา 1 วัน หรือ

(3.3) การปรับเพิ่มวงเงินการทำธุรกรรมโอนเงินต่อวัน ให้สามารถโอนได้ตั้งแต่ 50,000 บาทขึ้นไป

(4) ให้ตรวจสอบการเปลี่ยนแปลงแก้ไขแอปพลิเคชันของบริการ Mobile Banking ในทันทีที่ผู้ใช้บริการเข้าใช้งานบริการดังกล่าวทุกครั้ง (anti-tampering) และไม่อนุญาตให้ผู้ใช้บริการใช้งานแอปพลิเคชันหากพบว่ามีการเปลี่ยนแปลงแก้ไขแอปพลิเคชัน

(5) ไม่อนุญาตให้แอปพลิเคชันของบริการ Mobile Banking ทำงานบนอุปกรณ์เคลื่อนที่ในขณะที่มีแอปพลิเคชันอื่นซึ่งมีพฤติกรรมการทำงานที่เสี่ยงจะก่อให้เกิดการสวมรอยทำธุรกรรมแทนผู้ใช้บริการกำลังทำงาน ได้แก่ แอปพลิเคชันที่ขอสิทธิช่วยเหลือคนพิการ (accessibility services) โดยไม่จำเป็น แอปพลิเคชันที่สามารถควบคุมอุปกรณ์เคลื่อนที่จากระยะไกลได้ (remote control) แอปพลิเคชันที่มีการปิดบังหรือขโมยข้อมูลที่แสดงบนหน้าจอของผู้ใช้งาน

4.2.2 การรู้จักลูกค้า (Know Your Customer: KYC) เพื่อป้องกันบัญชีม้า

สถาบันการเงินต้องมีกระบวนการรู้จักลูกค้า (Know Your Customer: KYC) เพื่อเปิดบัญชีเงินฝาก ทั้งในการแสดงตนของลูกค้า (Identification) และการพิสูจน์ตัวตนลูกค้า (Verification) เพื่อป้องกันการสวมรอยหรือขโมยข้อมูลไปใช้เปิดบัญชีม้า ดังนี้

(1) การแสดงตนของลูกค้า (Identification)

สถาบันการเงินต้องได้รับข้อมูลและเอกสารหลักฐานการแสดงตนที่บ่งชี้ถึงตัวลูกค้าตามประเภทของลูกค้า โดยปฏิบัติตามหลักเกณฑ์ของกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ซึ่งข้อมูลและเอกสารหลักฐานการแสดงตนดังกล่าวให้หมายรวมถึงข้อมูลและเอกสารอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

(2) การพิสูจน์ตัวตนลูกค้า (Verification)

สถาบันการเงินต้องนำข้อมูลและเอกสารหลักฐานการแสดงตนของลูกค้าตามข้อ 4.2.2 (1) มาตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบัน รวมถึงต้องพิสูจน์ว่าเป็นลูกค้ารายนั้นจริง โดยให้สถาบันการเงินถือปฏิบัติตามหลักเกณฑ์การพิสูจน์ตัวตนลูกค้า ดังนี้

(2.1) การพิสูจน์ตัวตนลูกค้าด้วยสถาบันการเงินเอง

(2.1.1) การพิสูจน์ตัวตนลูกค้าแบบพบเห็นลูกค้าต่อหน้า (Face-to-Face)

ในการพิสูจน์ตัวตนลูกค้าแบบพบเห็นลูกค้าต่อหน้า (Face-to-Face) สถาบันการเงินจะเป็นผู้ดำเนินการตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูลและเอกสารหลักฐานการแสดงตนที่ได้รับจากการระบุตัวตนหรือการแสดงตนของลูกค้า รวมถึงพิสูจน์ว่าเป็นลูกค้าหรือบุคคลที่ได้รับมอบอำนาจทอดสุดท้ายจากนิติบุคคล (หากมี) รายนั้นจริง โดยข้อมูลที่ใช้พิสูจน์ตัวตนลูกค้าต้องได้จากแหล่งข้อมูลที่น่าเชื่อถือ เช่น กรณีการใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์ (Smart Card) เป็นเอกสารหลักฐานการแสดงตน สถาบันการเงินต้องตรวจสอบข้อมูลจากเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ (Smart Card Reader) และตรวจสอบสถานะของบัตรประจำตัวประชาชนผ่านระบบการตรวจสอบทางอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ นอกจากนี้ สถาบันการเงินอาจพิจารณานำเทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของลูกค้า (Biometric Comparison) มาเพิ่มประสิทธิภาพในการพิสูจน์ตัวตนลูกค้าได้ กรณีการใช้เอกสารหลักฐานการแสดงตนอื่น ให้ปฏิบัติตามหลักเกณฑ์ของกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน

(2.1.2) การพิสูจน์ตัวตนลูกค้าแบบไม่พบเห็นลูกค้าต่อหน้า (Non Face-to-Face)

ในการพิสูจน์ตัวตนลูกค้าแบบไม่พบเห็นลูกค้าต่อหน้า (Non Face-to-Face) สถาบันการเงินจะต้องตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูลและเอกสารหลักฐานการแสดงตนที่ได้จากการแสดงตนของลูกค้า รวมถึงพิสูจน์ว่าเป็นลูกค้าหรือบุคคลที่ได้รับมอบอำนาจทอดสุดท้ายจากนิติบุคคล (หากมี) รายนั้นจริง จากแหล่งข้อมูลที่น่าเชื่อถือ เช่น กรณีการใช้บัตรประจำตัวประชาชนเป็นเอกสารหลักฐานการแสดงตน สถาบันการเงินต้องตรวจสอบข้อมูลจากเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์และตรวจสอบสถานะของบัตรประจำตัวประชาชนผ่านระบบการตรวจสอบทางอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ นอกจากนั้น สถาบันการเงินต้องถ่ายรูปลูกค้า รวมถึงต้องใช้เทคโนโลยีเพื่อพิสูจน์ความเป็นบุคคลและสังเกตพฤติกรรมลูกค้า (เช่น เทคโนโลยี Liveness Detection) และเทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของลูกค้า (Biometric Comparison) เพื่อพิสูจน์ว่าเป็นลูกค้ารายนั้นจริงทดแทนการพบเห็นลูกค้าต่อหน้า

(2.2) การพิสูจน์ตัวตนลูกค้าด้วยระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

สถาบันการเงินสามารถตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูลและเอกสารหลักฐานการแสดงตน รวมถึงการพิสูจน์ว่าเป็นลูกค้า

หรือบุคคลที่ได้รับมอบอำนาจทอดสุดท้ายจากนิติบุคคล (หากมี) รายนั้นจริง ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ผ่าน National Digital ID Platform (NDID Platform) หรือระบบอื่นที่สถาบันการเงินได้หารือและเห็นร่วมกันกับ ธปท. ว่ามีมาตรฐานในการพิสูจน์ตัวตนที่ไม่ต่ำกว่าการพิสูจน์ตัวตนลูกค้าด้วยสถาบันการเงินเองแทนการพิสูจน์ตัวตนลูกค้าหรือประกอบการพิสูจน์ตัวตนลูกค้าตามข้อ 4.2.2 (2.1) ข้างต้นก็ได้

4.2.3 การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า

สถาบันการเงินต้องประเมินความเสี่ยงลูกค้าและตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าตามหลักเกณฑ์ของกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ดังนี้

(1) เมื่อปรากฏว่าลูกค้ารายใดเป็นเจ้าของบัญชีม้าดำ หรือบัญชีม้าเทาเข้ม หรือบัญชีม้าเทาอ่อนซึ่งถือได้ว่าเป็นปัจจัยที่อาจทำให้เกิดความเสี่ยงสูงเกี่ยวกับตัวลูกค้า ทั้งกรณีความสัมพันธ์ทางธุรกิจดำเนินไปอย่างผิดปกติ และกรณีลูกค้าอาจเกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี ซึ่งพฤติการณ์ของการกระทำความผิดดังกล่าวเป็นความผิดมูลฐานตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ให้สถาบันการเงินกำหนดระดับความเสี่ยงของลูกค้าที่เป็นเจ้าของบัญชีม้าดำ บัญชีม้าเทาเข้ม และบัญชีม้าเทาอ่อน เป็นลูกค้าที่มีความเสี่ยงด้านการฟอกเงินในระดับความเสี่ยงสูง ทั้งนี้ เพื่อเป็นการป้องกันอาชญากรรมทางเทคโนโลยี

(2) การตรวจสอบเพื่อทราบข้อเท็จจริงของลูกค้าที่มีความเสี่ยงสูงข้างต้นในระดับเข้มข้นตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ให้สถาบันการเงินหาข้อมูลจากแหล่งข้อมูลที่น่าเชื่อถือหรือขอข้อมูลเพิ่มเติมจากลูกค้าเกี่ยวกับแหล่งที่มาของเงินหรือทรัพย์สิน แหล่งที่มาของฐานะความมั่นคง หรือวัตถุประสงค์ในการทำธุรกรรมแต่ละครั้ง รวมถึงข้อมูลเกี่ยวกับการประกอบกิจการของลูกค้า อาชีพ ชื่อและสถานที่ตั้งของที่ทำงาน หรือลายมือชื่อของผู้ทำธุรกรรม

(3) ในกรณีที่สถาบันการเงินไม่สามารถตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าตามข้อ 4.2.3 (2) ข้างต้นได้ ให้สถาบันการเงินดำเนินการตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน กล่าวคือ ปฏิเสธการสร้างความสัมพันธ์ทางธุรกิจ ไม่ทำธุรกรรม ยุติความสัมพันธ์ทางธุรกิจ หรือไม่ทำธุรกรรมเป็นครั้งคราวกับลูกค้าดังกล่าว โดยในการดำเนินการข้างต้นให้สถาบันการเงินพิจารณาดำเนินการในแนวทางที่เป็นประโยชน์ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และต้องไม่เป็นไปในแนวทางสนับสนุนหรือเป็นประโยชน์ต่อการก่ออาชญากรรมทางเทคโนโลยี ทั้งนี้ การดำเนินการดังกล่าวให้มีรายละเอียดที่แตกต่างกันตามประเภทของบัญชีม้าดำ บัญชีม้าเทาเข้ม และบัญชีม้าเทาอ่อนตามที่กำหนดในข้อ 4.2.4 (4)

4.2.4 การจำกัดความเสียหายและการจัดการบัญชีม้า

สถาบันการเงินต้องดำเนินการจำกัดความเสียหายและจัดการบัญชีม้า ดังนี้

(1) จัดให้มีการแจ้งเตือนลูกค้าที่เป็นบุคคลธรรมดาผ่านช่องทางใดช่องทางหนึ่งทันทีเมื่อมีเงินออกจากบัญชีเงินฝากจากการทำธุรกรรมผ่านช่องทางดิจิทัล โดยไม่เรียกเก็บค่าใช้จ่าย เช่น การแจ้งเตือนผ่านบริการ Mobile Banking (In-App Notifications) บัญชีทางการบนแพลตฟอร์มส่งข้อความ (เช่น LINE Official Account) ข้อความสั้น (SMS) อีเมล

(2) ให้สถาบันการเงินระงับการทำธุรกรรม ยกเลิกการระงับการทำธุรกรรม แจ้งสถาบันการเงินหรือผู้ประกอบธุรกิจที่รับโอนถัดไป รวมทั้งนำข้อมูลเข้าสู่ระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล ตามข้อปฏิบัติที่ศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) กำหนด

(3) กรณีได้รับแจ้งรายชื่อบุคคลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยีตามประกาศในมาตรา 8/5 (6) แห่งพระราชกำหนด จากศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) ให้สถาบันการเงินดำเนินการตามมาตรา 4/2 แห่งพระราชกำหนด โดยในการดำเนินการตามมาตรา 4/2 ข้างต้น ให้สถาบันการเงินพิจารณาดำเนินการในแนวทางที่เป็นประโยชน์ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และต้องไม่เป็นไปในแนวทางสนับสนุนหรือเป็นประโยชน์ต่อการก่ออาชญากรรมทางเทคโนโลยี และหากศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) กำหนดข้อปฏิบัติเกี่ยวกับมาตรา 4/2 แห่งพระราชกำหนด ให้สถาบันการเงินปฏิบัติตามข้อปฏิบัติของศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) นั้น

(4) เมื่อสถาบันการเงินได้ปรับระดับความเสี่ยงลูกค้าเป็นลูกค้าที่มีความเสี่ยงสูงตามข้อ 4.2.3 แล้ว ให้สถาบันการเงินดำเนินการตามประเภทของบัญชีม้าดังนี้

(4.1) บัญชีม้าดำ

(4.1.1) ไม่ทำธุรกรรมกับลูกค้า โดยระงับการทำธุรกรรมทั้งไม่ให้เงินเข้าและออกจากบัญชีเงินฝากทุกบัญชีของลูกค้านั้นทุกช่องทางให้บริการ เว้นแต่บัญชีที่สถาบันการเงินได้ดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าที่มีความเสี่ยงสูงในระดับเข้มข้น (Enhanced Customer Due Diligence: EDD) โดยให้ถือว่าเอกสารจากกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (สอท.) เป็นข้อมูลและหลักฐานสำคัญที่บ่งชี้ได้ว่าเป็นบัญชีที่ลูกค้าสามารถใช้เป็นบัญชีเพื่อการดำรงชีพ สถาบันการเงินจึงทำธุรกรรมกับลูกค้าเฉพาะบัญชีนั้นได้

(4.1.2) ปฏิเสธการเปิดบัญชีเงินฝากให้กับลูกค้านั้น เว้นแต่สถาบันการเงินจะได้ดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าที่มีความเสี่ยงสูงในระดับเข้มข้น (Enhanced Customer Due Diligence: EDD) โดยให้ถือว่าเอกสารจากกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (สอท.) เป็นข้อมูลและหลักฐานสำคัญที่บ่งชี้ได้ว่าให้เปิดบัญชีเงินฝากเพื่อการดำรงชีพได้

ทั้งนี้ หากสำนักงานป้องกันและปราบปรามการฟอกเงินเพิกถอนรายชื่อลูกค้ารายใดออกจากรายชื่อบุคคลที่มีความเสี่ยงสูงซึ่งควรได้รับการเฝ้าระวังอย่างใกล้ชิดตามกฎกระทรวงการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า พ.ศ. 2563 ให้สถาบันการเงินสามารถทำธุรกรรมและเปิดบัญชีกับลูกค้ารายดังกล่าวได้

(4.2) บัญชีม้าเทาเข้ม

(4.2.1) ไม่ทำธุรกรรมกับลูกค้า โดยระงับการทำธุรกรรมทั้งไม่ให้เงินเข้าและออกจากบัญชีเงินฝากทุกบัญชีของลูกค้านั้นทุกช่องทางให้บริการ เว้นแต่บัญชีที่สถาบันการเงินได้ดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าที่มีความเสี่ยงสูงในระดับเข้มข้น (Enhanced Customer Due Diligence: EDD) โดยให้ถือว่าเอกสารจากกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (สอท.) เป็นข้อมูลและหลักฐานสำคัญที่บ่งชี้ได้ว่าเป็นบัญชีที่ลูกค้าสามารถใช้เป็นบัญชีเพื่อการดำรงชีพ สถาบันการเงินจึงทำธุรกรรมกับลูกค้าเฉพาะบัญชีนั้นได้

(4.2.2) ปฏิเสธการเปิดบัญชีเงินฝากให้กับลูกค้านั้น เว้นแต่สถาบันการเงินจะได้ดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าที่มีความเสี่ยงสูงในระดับเข้มข้น (Enhanced Customer Due Diligence: EDD) โดยให้ถือว่าเอกสารจากกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (สอท.) เป็นข้อมูลและหลักฐานสำคัญที่บ่งชี้ได้ว่าให้เปิดบัญชีเงินฝากเพื่อการดำรงชีพได้

ทั้งนี้ ให้ดำเนินการจนกว่าจะปลดรายชื่อลูกค้าจากระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล

(4.3) บัญชีม้าเทาอ่อน

(4.3.1) ไม่ทำธุรกรรมกับลูกค้า โดยระงับการทำธุรกรรมทั้งไม่ให้เงินเข้าและออกจากบัญชีเงินฝากทุกบัญชีของลูกค้านั้นทุกช่องทางให้บริการ เว้นแต่บัญชีที่สถาบันการเงินได้ดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าที่มีความเสี่ยงสูงในระดับเข้มข้น (Enhanced Customer Due Diligence: EDD) ตามข้อ 4.2.3 (2) แบบพบหน้าลูกค้าที่สาขาของสถาบันการเงินแล้วพบว่ามีข้อมูลและหลักฐานที่สามารถชี้แจงได้ว่าบัญชีใดไม่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี สถาบันการเงินจึงทำธุรกรรมกับลูกค้าเฉพาะบัญชีนั้นได้

(4.3.2) ปฏิเสธการเปิดบัญชีเงินฝากให้กับลูกค้านั้น เว้นแต่สถาบันการเงินจะได้ดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าที่มีความเสี่ยงสูงในระดับเข้มข้น (Enhanced Customer Due Diligence: EDD) ตามข้อ 4.2.3 (2) แบบพบหน้าลูกค้าที่สาขาของสถาบันการเงินแล้วพบว่ามีข้อมูลและหลักฐานที่สามารถชี้แจงได้ว่าลูกค้านั้นไม่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี

ทั้งนี้ ให้ดำเนินการจนกว่าจะปลดรายชื่อลูกค้าจากระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล

หากบุคคลที่เป็นเจ้าของบัญชีม้าดำ บัญชีม้าเทาเข้ม และบัญชีม้าเทาอ่อนรายใดได้รับการประกาศรายชื่อโดยศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) ว่าเป็นบุคคลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยีตามมาตรา 8/5 (6) ให้สถาบันการเงินดำเนินการตามข้อ 4.2.4 (3) แทนการดำเนินการตามข้อ 4.2.4 (4) ตามแต่กรณี

4.2.5 กระบวนการรับแจ้งเหตุที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี

สถาบันการเงินต้องจัดให้มีช่องทางติดต่อเร่งด่วน (hotline) ทางโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ที่ลูกค้าสามารถติดต่อเจ้าหน้าที่ของสถาบันการเงินเพื่อแจ้งเหตุที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีได้ทั้งในและนอกเวลาทำการ

5. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ 25 กรกฎาคม 2568

(นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

งานจัดการภัยทุจริตทางการเงิน
โทรศัพท์ 0 2283 6168, 0 2283 6176
อีเมล antifraud-policy@bot.or.th

คำถาม – คำตอบแนบท้ายประกาศธนาคารแห่งประเทศไทย
เรื่อง มาตรฐานและมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีสำหรับสถาบันการเงิน
ลงวันที่ 25 กรกฎาคม 2568

ข้อ	คำถาม	แนวคำตอบ
1.	การดำเนินการกับลูกค้าตามมาตรฐานและมาตรการต่าง ๆ ที่กำหนดในหลักเกณฑ์ฉบับนี้ ครอบคลุมถึงการดำเนินการกับบุคคลที่ได้รับมอบอำนาจจากลูกค้าเพื่อทำธุรกรรมแทน และบุคคลที่เกี่ยวข้องกับลูกค้าที่เป็นนิติบุคคล (เช่น กรรมการ ผู้รับมอบอำนาจ ทอดสุดท้าย ผู้ได้รับผลประโยชน์ที่แท้จริง) หรือไม่	การดำเนินการกับลูกค้าตามคำจำกัดความที่กำหนดในหลักเกณฑ์ข้อ 4.1 ทั้งที่เป็นบุคคลธรรมดาหรือนิติบุคคลนั้น ไม่ครอบคลุมถึงบุคคลที่ได้รับมอบอำนาจจากลูกค้าและบุคคลที่เกี่ยวข้องกับลูกค้าที่เป็นนิติบุคคลนั้น เว้นแต่กรณีที่หลักเกณฑ์ฉบับนี้ได้กำหนดไว้เป็นการเฉพาะ เช่น การพิสูจน์ตัวตนบุคคลที่ได้รับมอบอำนาจทอดสุดท้ายจากลูกค้าที่เป็นนิติบุคคล (หากมี) ตามหลักเกณฑ์ข้อ 4.2.2
2.	กรณีธนาคารพาณิชย์ไร้สาขาดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าที่มีความเสี่ยงสูงในระดับเข้มข้น (Enhanced Customer Due Diligence: EDD) แบบพบหน้าลูกค้าที่สาขาของสถาบันการเงินตามที่กำหนดในหลักเกณฑ์ข้อ 4.2.4 (4.3.1) ไม่ได้ เนื่องจากไม่สามารถจัดตั้งสาขาได้ ธนาคารพาณิชย์ไร้สาขาต้องดำเนินการอย่างไร	ธนาคารพาณิชย์ไร้สาขาสามารถดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าที่มีความเสี่ยงสูงในระดับเข้มข้นกับลูกค้าที่เป็นเจ้าของบัญชีม้าเทาอ่อนได้ด้วยการโทรศัพท์ผ่านวิดีโอ (video call) ผ่าน Mobile Banking ของธนาคารพาณิชย์ไร้สาขา ซึ่งต้องสามารถยืนยันตัวตนว่าเป็นลูกค้ารายนั้นจริง และสังเกตพฤติกรรมของลูกค้าได้เทียบเท่ากับการพบหน้าลูกค้าที่สาขาของสถาบันการเงิน ทั้งนี้ การดำเนินการข้างต้นต้องมีความปลอดภัยเท่าทันความเสี่ยงจากภัยคุกคามทางไซเบอร์และภัยทุจริตทางการเงินที่มีการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (unauthorized payment fraud) สอดคล้องกับหลักเกณฑ์ว่าด้วยการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงิน