ธนาคารแห่งประเทศไทย
BANK OF THAILAND

เอกสารรับฟังความคิดเห็น

(ร่าง) หลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล
(Digital Fraud Management)

งานจัดการภัยทุจริตทางการเงิน
ธนาคารแห่งประเทศไทย
มีนาคม 2568

(ร่าง) ประกาศธนาคารแห่งประเทศไทย

ที่ ธปท. xx / 2568

เรื่อง หลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management)

---

1. เหตุผลในการออกประกาศ

ภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงินมีหลากหลายรูปแบบ ไม่ว่าจะเป็นการสวมรอยทำธุรกรรมแทนลูกค้า (unauthorized payment fraud) หรือการหลอกลวงประชาชนให้หลงเชื่อและโอนเงินไปให้มิจฉาชีพด้วยตนเอง (authorized payment fraud) ซึ่งก่อให้เกิดความเสียหายต่อประชาชนในวงกว้าง และกระทบต่อระบบเศรษฐกิจโดยรวม ที่ผ่านมาธนาคารแห่งประเทศไทยตระหนักถึงความสำคัญในการบริหารจัดการภัยทุจริตดิจิทัลดังกล่าว จึงได้ออกหลักเกณฑ์และมาตรการต่าง ๆ ให้ผู้ให้บริการทางการเงินถือปฏิบัติมาอย่างต่อเนื่อง โดยล่าสุดได้ออกหลักเกณฑ์เพื่อยกระดับการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ เพื่อเป็นการป้องกันประชาชนจากการตกเป็นเหยื่อของมิจฉาชีพในรูปแบบ unauthorized payment fraud อย่างไรก็ตาม ปัจจุบันมิจฉาชีพมีการใช้รูปแบบ วิธีการ และเทคนิคที่มีความหลากหลายมากยิ่งขึ้น โดยเฉพาะรูปแบบ authorized payment fraud ที่ยังคงเป็นปัญหาสำคัญของประเทศไทย รวมถึงมีการใช้บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ เป็นเครื่องมือในการรับเงินและถ่ายโอนเงินที่ได้จากการกระทำความผิด ส่งผลให้ประชาชนจำนวนมากยังคงได้รับความเดือดร้อนต้องสูญเสียเงินให้กับมิจฉาชีพเป็นมูลค่ามหาศาล

ธนาคารแห่งประเทศไทยจึงยกระดับหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management) ให้ผู้ให้บริการทางการเงินใช้เป็นแนวทางในการบริหารจัดการภัยทุจริตดิจิทัลตั้งแต่ต้นจนจบกระบวนการ (end-to-end) โดยเริ่มตั้งแต่การป้องกัน ติดตามและตรวจจับ จัดการและแก้ไขเมื่อเกิดเหตุภัยทุจริตดิจิทัล รวมทั้งดูแลลูกค้าที่ได้รับผลกระทบ เพื่อให้การบริหารจัดการภัยทุจริตดิจิทัลเป็นไปอย่างมีประสิทธิผล สอดรับกับสภาพแวดล้อมทางการเงินที่เปลี่ยนแปลงไป ช่วยป้องกันและลดความเสียหายที่จะเกิดขึ้นกับประชาชน และรักษาความเชื่อมั่นในระบบสถาบันการเงินและระบบการชำระเงินของประเทศ

2. อำนาจตามกฎหมาย

2.1 อาศัยอำนาจตามความในมาตรา 39 มาตรา 41 และมาตรา 71 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 และที่แก้ไขเพิ่มเติม ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัลให้สถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

2.2 อาศัยอำนาจตามความในมาตรา 120/1 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 และที่แก้ไขเพิ่มเติม ธนาคารแห่งประเทศไทยโดยความเห็นชอบของรัฐมนตรีว่าการกระทรวงการคลังออกหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัลให้สถาบันการเงินเฉพาะกิจถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

2.3 อาศัยอำนาจตามความในมาตรา 24 และมาตรา 26 แห่งพระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัลให้ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับและผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

3. แนวนโยบายและหนังสือเวียนที่ยกเลิก

3.1 แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ลงวันที่ 29 มีนาคม 2566

3.2 หนังสือเวียนที่ ธปท.ฝตท.(01) ว. 384/2567 เรื่อง การเพิ่มความเข้มงวดในการจัดการบัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์ในกรณีลูกค้ามีความเสี่ยงสูงหรือใช้บัญชีที่มีลักษณะหรือพฤติกรรมผิดปกติ ลงวันที่ 31 พฤษภาคม 2567

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ให้บริการทางการเงิน ดังต่อไปนี้

4.1 สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

4.2 สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

4.3 ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับและผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงินทุกแห่ง

5. เนื้อหา

5.1 คำจำกัดความ

ในประกาศฉบับนี้

“ผู้ให้บริการทางการเงิน” หมายความว่า สถาบันการเงิน สถาบันการเงินเฉพาะกิจที่ให้บริการรับฝากเงินจากประชาชน ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ

“ลูกค้า” หมายความว่า บุคคลธรรมดา นิติบุคคล หรือบุคคลที่มีการตกลงกันทางกฎหมาย ซึ่งสร้างความสัมพันธ์ทางธุรกิจหรือทำธุรกรรมกับผู้ให้บริการทางการเงิน

“บัญชี” หมายความว่า บัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์

“บัญชีเงินฝาก” หมายความว่า บัญชีเพื่อการรับฝากเงินหรือการรับเงินจากประชาชนของสถาบันการเงินและสถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“บัญชีเงินอิเล็กทรอนิกส์” หมายความว่า บัญชีบัตรอิเล็กทรอนิกส์ที่ผู้ประกอบธุรกิจออกให้แก่ลูกค้า เพื่อใช้ชำระค่าสินค้า ค่าบริการ หรือค่าอื่นใดแทนการชำระด้วยเงินสด ตามมูลค่าของเงินที่ลูกค้าชำระเงินให้แก่ผู้ประกอบธุรกิจไว้ล่วงหน้า

“การทำธุรกรรมทางการเงิน” หมายความว่า การทำธุรกรรมทางการเงินที่ผู้ให้บริการทางการเงินให้บริการ เช่น การเปิดบัญชี การสมัครใช้บริการ การฝากเงิน การถอนเงิน การโอนเงิน และการชำระค่าสินค้าและบริการ โดยผ่านช่องทางการให้บริการครอบคลุม สาขาทั่วไป สาขาอิเล็กทรอนิกส์ ช่องทางดิจิทัล หรือช่องทางให้บริการอื่นที่ธนาคารแห่งประเทศไทยอนุญาตเพิ่มเติม ทั้งที่เป็นการทำธุรกรรมทางการเงินผ่านบัตร บริการเงินอิเล็กทรอนิกส์ หรือผ่านสื่ออื่น เช่น QR Code (Quick Response Code)

“บัญชีม้า” หมายความว่า บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ ซึ่งถูกมิจฉาชีพนำมาใช้เป็นเครื่องมือในการรับเงินและถ่ายโอนเงินที่ได้มาจากการกระทำความผิด

“มาตรฐานอุตสาหกรรม (Industry Standards)” หมายความว่า มาตรฐานอุตสาหกรรมที่ผู้ให้บริการทางการเงินได้ร่วมกันจัดทำเพื่อเป็นแนวปฏิบัติในการบริหารจัดการภัยทุจริตดิจิทัล

5.2 หลักการ

ผู้ให้บริการทางการเงินต้องให้ความสำคัญกับการบริหารจัดการภัยทุจริตดิจิทัลอย่างเหมาะสมและทันกาล เพื่อช่วยป้องกันและลดความเสียหายที่จะเกิดขึ้นกับประชาชนได้อย่างมีประสิทธิผล โดยต้องสร้างความสมดุลระหว่างความสะดวกและความปลอดภัยในการทำธุรกรรมทางการเงิน และคำนึงถึงการคุ้มครองลูกค้าอย่างเป็นธรรม

5.3 หลักเกณฑ์

ผู้ให้บริการทางการเงินที่เป็นธนาคารพาณิชย์ สถาบันการเงินเฉพาะกิจที่ให้บริการรับฝากเงินจากประชาชน และผู้ให้บริการทางการเงินที่ให้บริการเกี่ยวข้องกับบัญชีเงินอิเล็กทรอนิกส์เฉพาะที่ให้บริการโอนเงินไปยังบัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์ที่ให้บริการโดยผู้ให้บริการทางการเงินอื่นได้ ต้องถือปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ทุกข้อ

สำหรับผู้ให้บริการทางการเงินอื่นนอกเหนือจากที่กล่าวข้างต้น ธนาคารแห่งประเทศไทยสนับสนุนให้ผู้ให้บริการทางการเงินนำหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ไปปรับใช้ตามความเหมาะสม ทั้งนี้ ให้ขึ้นกับขอบเขตการประกอบธุรกิจ ประเภทของผลิตภัณฑ์ และช่องทางการให้บริการ

5.3.1 การกำหนดนโยบายและการกำกับดูแลการบริหารจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

คณะกรรมการและผู้บริหารระดับสูงของผู้ให้บริการทางการเงินต้องกำกับดูแลให้ผู้ให้บริการทางการเงินมีการบริหารจัดการเหตุการณ์ภัยทุจริตดิจิทัลที่เหมาะสมกับรูปแบบและผลกระทบของภัยทุจริตดิจิทัลที่เกิดขึ้น และมีการแก้ไขสถานการณ์ที่ทันกาล เพื่อป้องกันและลดความเสียหายที่จะเกิดขึ้นกับประชาชน ตั้งแต่ต้นจนจบกระบวนการ (end-to-end) โดยเริ่มตั้งแต่การป้องกัน ติดตามและตรวจจับ จัดการและแก้ไขเมื่อเกิดเหตุภัยทุจริตดิจิทัล รวมทั้งดูแลลูกค้าที่ได้รับผลกระทบ โดยกำหนดให้เป็นความเสี่ยงสำคัญที่องค์กรต้องมีการบริหารจัดการร่วมกันแบบบูรณาการ โดยผู้ให้บริการทางการเงินต้องดำเนินการ ดังนี้

(1) กำหนดให้มีคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทำหน้าที่กำหนดนโยบายและกำกับดูแลอย่างชัดเจน เพื่อให้องค์กรให้ความสำคัญและมีแนวทางบริหารจัดการภัยทุจริตดิจิทัลที่เหมาะสม ทันกาล และมีประสิทธิผลอย่างต่อเนื่อง สอดรับกับบริบทของปัญหาภัยทุจริตในแต่ละช่วงเวลา และสามารถลดความเสียหายที่จะเกิดขึ้นกับประชาชนได้ทันท่วงที

(2) กำหนดนโยบายการบริหารจัดการภัยทุจริตดิจิทัลที่ชัดเจนเป็นลายลักษณ์อักษร ซึ่งได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย รวมทั้งจัดให้มีการทบทวนและปรับปรุงนโยบายอย่างสม่ำเสมอ โดยเฉพาะเมื่อมีเหตุการณ์หรือการเปลี่ยนแปลงที่ส่งผลกระทบต่อประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัลอย่างมีนัยสำคัญ หรืออย่างน้อยปีละ 1 ครั้ง โดยนโยบายดังกล่าวต้องครอบคลุมอย่างน้อย ดังนี้

(2.1) บทบาทหน้าที่ของคณะกรรมการหรือผู้บริหารระดับสูงที่กำกับดูแลและหน่วยงานที่รับผิดชอบ เพื่อผลักดันให้มีการบริหารจัดการภัยทุจริตดิจิทัลที่มีประสิทธิผล โดยครอบคลุมกระบวนการแบบ end-to-end รวมทั้งประเมินความพร้อมขององค์กร ทั้งในด้านบุคลากร กระบวนการ เทคโนโลยีและเครื่องมือที่ใช้ในการจัดการภัยทุจริตดิจิทัลอย่างสม่ำเสมอ

(2.2) แนวทางและกระบวนการบริหารจัดการภัยทุจริตดิจิทัล ตั้งแต่ต้นจนจบกระบวนการ (end-to-end) เพื่อให้การบริหารจัดการภัยทุจริตดิจิทัลเป็นไปอย่างมีประสิทธิผล

(2.3) การติดตามและวัดประสิทธิผลของการจัดการภัยทุจริตดิจิทัลอย่างต่อเนื่อง เพื่อทบทวนแนวทางและกระบวนการให้เหมาะสมกับสถานการณ์อยู่เสมอ

ทั้งนี้ นโยบายดังกล่าวต้องสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง บริบทของปัญหาภัยทุจริตดิจิทัลในแต่ละช่วงเวลา และสอดคล้องกับมาตรฐานอุตสาหกรรม (Industry Standards) ซึ่งผ่านการหารือกับธนาคารแห่งประเทศไทยแล้ว ตลอดจนจัดให้มีการสื่อสารเผยแพร่นโยบายและแนวปฏิบัติเพื่อให้ทุกฝ่ายงานในองค์กรนำไปปฏิบัติได้อย่างเหมาะสม

(3) กำหนดเป้าหมายและตัวชี้วัดในการประเมินประสิทธิผลของการจัดการภัยทุจริตดิจิทัลที่ชัดเจนและวัดผลได้จริง ครอบคลุมกระบวนการแบบ end-to-end และต้องปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับรูปแบบภัยทุจริตดิจิทัลที่เปลี่ยนแปลงไป

(4) ออกแบบและพัฒนาระบบงาน กระบวนการ และผลิตภัณฑ์หรือบริการทางการเงิน โดยคำนึงถึงเหตุการณ์และปัจจัยความเสี่ยงที่อาจทำให้เกิดภัยทุจริตดิจิทัล เช่น การยกระดับกระบวนการรู้จักลูกค้าเพื่อป้องกันการสวมรอยสมัครใช้บริการทางการเงินแทนลูกค้าตัวจริง การยกระดับการยืนยันตัวตนเพื่อป้องกันการถูกผู้ไม่ประสงค์ดีทำธุรกรรมทางการเงินโดยไม่ได้รับอนุญาตแทนลูกค้าตัวจริง การกำหนดเพดานวงเงินการทำธุรกรรมสูงสุดต่อวันเพื่อป้องกันและลดความเสียหายที่จะเกิดขึ้น

นอกจากนี้ ผู้ให้บริการทางการเงินต้องสื่อสารและพัฒนาองค์ความรู้ของบุคลากรในองค์กรเกี่ยวกับการบริหารจัดการภัยทุจริตดิจิทัลอย่างต่อเนื่อง เพื่อให้พนักงานทุกระดับมีความรู้ความเข้าใจที่เพียงพอในการกำกับดูแลและการบริหารจัดการภัยทุจริตดิจิทัลรูปแบบใหม่ ๆ ที่อาจเกิดขึ้น

(5) ติดตามและประเมินประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัล รวมทั้งปรับปรุงระบบงาน กระบวนการ และผลิตภัณฑ์หรือบริการทางการเงิน ให้ครอบคลุมรูปแบบของภัยทุจริตที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง เพื่อให้สามารถตรวจจับและจัดการธุรกรรมที่มีความผิดปกติได้ทันท่วงที โดยต้องจัดให้มีการรายงานเรื่องดังกล่าวต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายอย่างต่อเนื่อง

นอกจากนี้ หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง หน่วยงานที่ทำหน้าที่กำกับการปฏิบัติตามกฎเกณฑ์ และหน่วยงานที่ทำหน้าที่ตรวจสอบภายใน ต้องมีส่วนร่วมในการผลักดันให้องค์กรมีกระบวนการควบคุมดูแลความเสี่ยงที่ดี เพื่อให้การบริหารจัดการภัยทุจริตดิจิทัลขององค์กรดำเนินการได้อย่างเหมาะสม และทันกาล

(6) สนับสนุนการจัดทำมาตรฐานอุตสาหกรรม (Industry Standards) โดยให้ครอบคลุมกระบวนการบริหารจัดการภัยทุจริตดิจิทัลที่จำเป็น เพื่อให้มั่นใจว่ากระบวนการบริหารจัดการขั้นต่ำมีมาตรฐานเดียวกัน โดยต้องผ่านการหารือร่วมกับธนาคารแห่งประเทศไทยก่อนนำมาใช้

5.3.2 กระบวนการจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

ผู้ให้บริการทางการเงินต้องจัดให้มีกรอบการดำเนินการบริหารจัดการภัยทุจริตดิจิทัลที่ชัดเจนตลอดวงจรการเป็นลูกค้า เริ่มตั้งแต่การสมัครหรือเปิดใช้บริการ การทำธุรกรรมทางการเงิน จนถึงการปิดบัญชีหรือยกเลิกการใช้บริการ ทั้งนี้ ให้ถือปฏิบัติตามมาตรฐานอุตสาหกรรม (Industry Standards) เป็นแนวทางขั้นต่ำ และครอบคลุมกระบวนการอย่างน้อย ดังนี้

(1) กระบวนการรู้จักลูกค้า (Know Your Customer: KYC) และการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (Customer Due Diligence: CDD)

ผู้ให้บริการต้องมีกระบวนการในการประเมินความเสี่ยงที่ลูกค้าอาจเข้าข่ายเป็นบัญชีม้า โดยต้องกำหนดกระบวนการรู้จักลูกค้าและการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าที่สอดคล้องกับระดับความเสี่ยงของลูกค้าตั้งแต่วันเปิดบัญชี และต้องติดตามและวิเคราะห์พฤติกรรมการทำธุรกรรมของลูกค้า รวมถึงทบทวนระดับความเสี่ยงของลูกค้าให้เป็นปัจจุบันอยู่เสมอ ทั้งนี้ สำหรับกรณีลูกค้ามีความเสี่ยงสูง ผู้ให้บริการทางการเงินต้องดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าในระดับเข้มข้น (enhanced CDD) เช่น ตรวจสอบแหล่งที่มาของเงินหรือทรัพย์สิน แหล่งที่มาของฐานะความมั่งคั่ง หรือวัตถุประสงค์ในการทำธุรกรรมในแต่ละครั้ง รวมถึงข้อมูลเกี่ยวกับการประกอบกิจการของลูกค้า อาชีพ ชื่อและสถานที่ตั้งของที่ทำงาน นอกจากนี้ ผู้ให้บริการทางการเงินต้องถือปฏิบัติตามกฎหมายและหลักเกณฑ์อื่นที่เกี่ยวข้องด้วย เช่น กฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน กฎหมายว่าด้วยการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง ประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การรู้จักลูกค้าสำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน หลักเกณฑ์การรับฝากเงินหรือการรับเงินจากประชาชนของสถาบันการเงินเฉพาะกิจ และหลักเกณฑ์การรู้จักลูกค้าสำหรับการเปิดใช้บริการเงินอิเล็กทรอนิกส์

ทั้งนี้ ผู้ให้บริการต้องมีกระบวนการยืนยันตัวตนลูกค้า (authentication) ที่รัดกุมและเหมาะสมกับระดับความเสี่ยงของธุรกรรม ผลิตภัณฑ์และบริการ รวมถึงช่องทางการให้บริการ

(2) การติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงิน (monitoring and detection)

ผู้ให้บริการทางการเงินต้องมีกระบวนการในการติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงินที่มีประสิทธิผลและเป็นลักษณะเชิงรุก ครอบคลุมรูปแบบของภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงินที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง โดยต้องสามารถประเมินระดับความเสี่ยงของบัญชีทั้งบัญชีของบุคคลที่คาดว่าจะได้รับความเสียหายและบุคคลที่มีความเสี่ยงเป็นบัญชีม้า รวมถึงตรวจจับธุรกรรมและบัญชีที่มีความผิดปกติได้อย่างทันท่วงที เพื่อให้มี

การจัดการที่เหมาะสมและทันกาล ซึ่งจะช่วยจำกัดความเสียหายและป้องกันไม่ให้ขยายตัวหรือลุกลามเป็นวงกว้าง ดังนี้

(2.1) จัดให้มีบุคลากร กระบวนการ และระบบในการติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงินอย่างเพียงพอเหมาะสม

(2.2) กำหนดเงื่อนไขในการติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงิน ทั้งธุรกรรมของบุคคลที่คาดว่าจะได้รับความเสียหายและบุคคลที่มีความเสี่ยงเป็นบัญชีม้า โดยต้องพิจารณาถึงปัจจัยต่าง ๆ ดังนี้

- รูปแบบของภัยทุจริตดิจิทัลที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง ทั้งที่เกิดขึ้นภายในประเทศไทยและในต่างประเทศ
- ช่องทางการให้บริการ เช่น สาขาทั่วไป สาขาอิเล็กทรอนิกส์ (เช่น เครื่องถอนเงินสดอัตโนมัติ (Automatic Teller Machine: ATM) หรือเครื่องฝากเงินอัตโนมัติ (Cash Deposit Machine: CDM)) และช่องทางดิจิทัล (เช่น การให้บริการทางอินเทอเน็ต (Internet banking) อุปกรณ์เคลื่อนที่ (mobile banking))
- ข้อมูลของลูกค้าที่สามารถใช้ประเมินความเสี่ยงและความผิดปกติของธุรกรรม เช่น ยอดเงินฝากในบัญชี พฤติกรรมการใช้บัญชี ข้อมูลพฤติกรรมต้องสงสัยที่ผู้ให้บริการทางการเงินตรวจพบเอง ข้อมูลเจ้าของหมายเลขโทรศัพท์เคลื่อนที่ ข้อมูลที่สามารถระบุพิกัดหรือตำแหน่งการทำธุรกรรมของลูกค้า และข้อมูลเชิงเทคนิคของอุปกรณ์ที่ใช้ทำธุรกรรม
- ข้อมูลจากภายนอก เช่น ข้อมูลที่ได้รับจากผู้ให้บริการทางการเงินแห่งอื่น ข้อมูลจากระบบ Central Fraud Registry (CFR) ข้อมูลจากสำนักงานป้องกันและปราบปรามการฟอกเงิน ข้อมูลจากสำนักงานตำรวจแห่งชาติ และข้อมูลจากแหล่งอื่น ๆ ที่น่าเชื่อถือที่สะท้อนความเสี่ยงของภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

ทั้งนี้ ผู้ให้บริการทางการเงินต้องทบทวนและปรับปรุงเงื่อนไข รวมทั้งกระบวนการในการตรวจจับอย่างสม่ำเสมอและเป็นลักษณะเชิงรุก (proactive detection) โดยนำระบบวิเคราะห์ข้อมูล (data analytics) มาใช้ เพื่อให้สามารถติดตามและตรวจจับความผิดปกติได้ดียิ่งขึ้น และอาจนำเทคโนโลยีใหม่ ๆ เช่น เทคโนโลยีปัญญาประดิษฐ์ (artificial intelligence) มาใช้เพิ่มประสิทธิผลร่วมด้วย เพื่อให้เท่าทันกับสถานการณ์และรูปแบบภัยทุจริตใหม่ ๆ อันจะช่วยให้ผู้ให้บริการทางการเงินสามารถระงับเหตุการณ์ภัยทุจริตดิจิทัลและป้องกันความเสียหายที่อาจเกิดขึ้นได้อย่างทันกาล

(3) การจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน (actions)

ผู้ให้บริการทางการเงินต้องมีกระบวนการป้องกัน จำกัด และระงับความเสียหายจากภัยทุจริตดิจิทัลอย่างรวดเร็ว เพียงพอและเหมาะสม สอดคล้องตามระดับความเสี่ยงของธุรกรรม ซึ่งประกอบด้วยกระบวนการป้องกันลูกค้าจากการถูกหลอกลวงจากมิจฉาชีพ รวมถึงการจัดการบัญชีม้า หรือบัญชีที่มีความเสี่ยงที่จะถูกใช้เป็นเครื่องมือของมิจฉาชีพ โดยอย่างน้อยต้องจัดให้มี

(3.1) การป้องกันและจำกัดความเสียหายให้แก่ลูกค้า

ผู้ให้บริการทางการเงินต้องจัดให้มีกระบวนการป้องกันและจำกัดความเสียหายแก่ลูกค้าที่เพียงพอและเหมาะสมตามระดับความเสี่ยงของการทำธุรกรรม เช่น การแจ้งเตือนที่สามารถกระตุกพฤติกรรม (nudge) ให้ลูกค้าเพิ่มความระมัดระวังในการทำธุรกรรมทางการเงินได้อย่างมีประสิทธิผล การหน่วงธุรกรรมเมื่อมีเหตุอันควรสงสัย การระงับธุรกรรมที่มีความเสี่ยงสูงเพื่อลดความเสียหายเมื่อลูกค้าถูกหลอกลวงจากมิจฉาชีพหรือถูกใช้เป็นเครื่องมือในการทำทุจริต

<u>ตัวอย่างการจัดการเพื่อป้องกันและจำกัดความเสียหาย</u>

- การแจ้งเตือนลูกค้าแบบทันที (real time) กรณีลูกค้าทำธุรกรรมที่มีความเสี่ยง เช่น การโอนเงินไปสู่บัญชีของบุคคลที่มีความเสี่ยงสูงหรือมีลักษณะหรือพฤติกรรมผิดปกติที่เข้าข่ายเป็นบัญชีม้าทุกประเภท
- การแจ้งเตือนการทำธุรกรรมผ่านช่องทางต่าง ๆ โดยไม่มีค่าใช้จ่าย เช่น การแจ้งเตือนผ่านบัญชีทางการ LINE อีเมล ข้อความสั้น (SMS)
- การหน่วงหรือระงับธุรกรรมเมื่อตรวจพบความผิดปกติในการเดินบัญชี เช่น การโอนเงินออกเป็นจำนวนมากภายในระยะเวลาที่รวดเร็ว (rapidly drained)
- การหน่วงธุรกรรม (cooling off period) กรณีมีการดำเนินการที่เกี่ยวข้องกับการใช้บริการทางการเงินที่มีความเสี่ยงสูง เช่น การติดตั้ง mobile banking บนอุปกรณ์เคลื่อนที่ใหม่ การโอนเงินครั้งแรกภายหลังการเปิดใช้บริการ mobile banking การเปลี่ยนการตั้งค่ารหัสผ่าน (password)
- การติดต่อหาลูกค้าเพื่อสอบถามผู้รับผลประโยชน์ที่แท้จริงและยืนยันการทำธุรกรรม (call back)

นอกจากนี้ ผู้ให้บริการทางการเงินต้องจัดให้มีระบบรองรับให้ลูกค้าสามารถบริหารความเสี่ยงจากการใช้บริการทางการเงินผ่านแอปพลิเคชันของผู้ให้บริการทางการเงิน และแก้ไขสถานการณ์หรือระงับความเสียหายเมื่อตกเป็นเหยื่อของมิจฉาชีพได้ด้วยตนเอง

ตัวอย่างระบบรองรับสำหรับลูกค้า mobile banking

- การตั้งค่าบัญชีหรือเงินในบัญชีไม่ให้ทำธุรกรรมผ่านช่องทางอิเล็กทรอนิกส์ (money lock)
- การระงับการใช้บริการ mobile banking ด้วยตนเอง (kill switch)

(3.2) การจัดการบัญชีที่อาจเข้าข่ายเป็นบัญชีม้า เพื่อจำกัดและระงับความเสียหาย

ผู้ให้บริการทางการเงินต้องดำเนินการจำกัดและระงับความเสียหายให้สอดคล้องกับระดับความเสี่ยงของบัญชีที่อาจเข้าข่ายเป็นบัญชีม้า หรือผลกระทบของความเสียหายได้อย่างเหมาะสมและทันกาล ทั้งนี้ การจำกัดและระงับความเสียหายสามารถดำเนินการได้หลายรูปแบบ เช่น การกำหนดวงเงินการทำธุรกรรมต่อวันให้เหมาะสมกับระดับความเสี่ยงของลูกค้า การระงับเงินเข้า การระงับเงินออก การระงับช่องทางอิเล็กทรอนิกส์ การปฏิเสธการสร้างความสัมพันธ์อาทิ การปฏิเสธการเปิดบัญชีใหม่ การไม่เสนอขายผลิตภัณฑ์อื่น ๆ

ตัวอย่างการจัดการบัญชีที่อาจเข้าข่ายเป็นบัญชีม้า

- การตั้งค่าวงเงินเริ่มต้นของการทำธุรกรรมต่อวันของบริการ mobile banking (set limit) ให้สอดคล้องกับระดับความเสี่ยงของลูกค้า
- การปฏิเสธการเปิดบัญชีใหม่สำหรับลูกค้าที่อาจเข้าข่ายเป็นบัญชีม้า ซึ่งผู้ให้บริการทางการเงินไม่สามารถดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าในระดับเข้มข้น (enhanced CDD) ได้

(4) การแก้ไขสถานการณ์และการดูแลลูกค้า (response)

ผู้ให้บริการทางการเงินต้องกำหนดกระบวนการแก้ไขสถานการณ์และดูแลลูกค้าเมื่อเกิดเหตุการณ์ภัยทุจริตดิจิทัลที่ชัดเจน รวดเร็ว และเป็นธรรม โดยอย่างน้อยต้องดำเนินการ ดังนี้

(4.1) การจัดให้มีช่องทางรับแจ้งเหตุการณ์ต้องสงสัยหรือเหตุการณ์ภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

ผู้ให้บริการทางการเงินต้องจัดให้มีช่องทางติดต่อเร่งด่วน (hotline) ทางโทรศัพท์ หรือวิธีการทางอิเล็กทรอนิกส์ที่ลูกค้าสามารถติดต่อได้โดยตรงแยกออกจากช่องทางให้บริการปกติ อย่างเพียงพอและต่อเนื่องทั้งในและนอกเวลาทำการ (24x7) เพื่อให้ลูกค้าสามารถแจ้งเหตุภัยทุจริตดิจิทัลได้โดยเร็ว ทั้งนี้ หลังได้รับแจ้งเหตุ ผู้ให้บริการทางการเงินต้องเร่ง

ดำเนินการตามกฎหมายและหลักเกณฑ์อื่นที่เกี่ยวข้องอย่างเคร่งครัด เพื่อลดความเสียหายที่อาจเกิดขึ้น และให้การติดตามตรวจสอบเหตุการณ์เป็นไปอย่างทันกาล

ตัวอย่างการจัดให้มีช่องทางรับแจ้งเหตุการณ์ต้องสงสัยหรือเหตุการณ์ภัยทุจริตดิจิทัล

- ระบบที่ลูกค้าสามารถแจ้งเหตุภัยทุจริตดิจิทัลได้ด้วยตนเอง ผ่านช่องทาง mobile banking application (self-report)

(4.2) การกำหนดระยะเวลาและข้อตกลงในการใช้บริการ (Service Level Agreement)

ผู้ให้บริการทางการเงินต้องกำหนดระยะเวลาและข้อตกลงในการใช้บริการเพื่อดูแลลูกค้าที่ได้รับผลกระทบจากความเสียหายที่เกิดขึ้นจากเหตุการณ์ภัยทุจริตให้ชัดเจน เช่น การแจ้งให้ลูกค้าทราบเมื่อเกิดเหตุการณ์ การติดต่อกลับลูกค้าอย่างรวดเร็วภายในเวลาที่เหมาะสมหลังได้รับแจ้งเหตุการณ์ที่เข้าข่ายภัยทุจริตดิจิทัลจากลูกค้า การช่วยเหลือและดูแลลูกค้า รวมถึงสื่อสารและทำความเข้าใจกับลูกค้าเกี่ยวกับปัญหาและผลกระทบที่เกิดขึ้นอย่างทันกาล

(4.3) การช่วยเหลือและดูแลลูกค้า

ผู้ให้บริการทางการเงินต้องมีกระบวนการการดูแลลูกค้าที่ได้รับผลกระทบจากการดำเนินการ เพื่อบริหารจัดการภัยทุจริตดิจิทัลอย่างเหมาะสม รวดเร็ว และเป็นธรรม ทั้งนี้ กรณีการจัดการภัยทุจริตดิจิทัลของผู้ให้บริการทางการเงินกระทบต่อลูกค้าที่ไม่มีส่วนเกี่ยวข้องกับการกระทำทุจริต ผู้ให้บริการทางการเงินต้องมีกระบวนการพิสูจน์ทราบว่าผู้เสียหายไม่เกี่ยวข้องกับการกระทำความผิดและจัดการแก้ไขปัญหาที่รวดเร็ว เช่น การยกเลิกการหน่วงธุรกรรม การปลดการระงับบัญชี ภายหลังพิสูจน์ได้ว่าลูกค้าไม่มีส่วนเกี่ยวข้องกับการกระทำความผิด

(4.4) การรายงานเหตุการณ์ภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน และการสื่อสารต่อสาธารณชน

ผู้ให้บริการทางการเงินต้องมีกระบวนการในการรายงานเหตุการณ์ภัยทุจริตดิจิทัลแก่คณะกรรมการหรือผู้บริหารระดับสูงที่มีหน้าที่รับผิดชอบ เหมาะสมตามระดับความรุนแรงของเหตุการณ์ ทั้งนี้ กรณีที่เกิดความเสียหายกับลูกค้าในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของผู้ให้บริการทางการเงิน ต้องรายงานเหตุการณ์ภัยทุจริตดิจิทัลให้ธนาคารแห่งประเทศไทยทราบโดยเร็วตามช่องทางที่กำหนด

นอกจากนี้ ในกรณีที่เกิดเหตุการณ์ภัยทุจริตดิจิทัลกับผู้ให้บริการทางการเงินหลายรายพร้อมกัน และส่งผลกระทบในวงกว้างต่อความเชื่อมั่นของระบบการเงินหรือระบบการชำระเงิน ผู้ให้บริการทางการเงิน สมาคมผู้ประกอบธุรกิจ และหน่วยงานอื่นที่เกี่ยวข้องควร

ร่วมกันสื่อสารเพื่อชี้แจงและทำความเข้าใจกับลูกค้าโดยเร็ว และกำหนดแนวทางช่วยเหลือและดูแลลูกค้าให้เป็นมาตรฐานเดียวกัน

5.3.3 การแลกเปลี่ยนข้อมูลระหว่างผู้ให้บริการทางการเงิน รวมทั้งหน่วยงานภาครัฐและหน่วยงานภายนอกที่เกี่ยวข้อง

ผู้ให้บริการทางการเงินต้องจัดให้มีกลไกการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับเหตุการณ์ภัยทุจริตดิจิทัลระหว่างผู้ให้บริการทางการเงินและหน่วยงานภายนอกที่เกี่ยวข้องที่สามารถส่งผ่านข้อมูลได้อย่างถูกต้องและรวดเร็ว เพื่อให้ผู้ให้บริการทางการเงินและหน่วยงานภายนอก สามารถร่วมกันบริหารการจัดการภัยทุจริตดิจิทัลได้อย่างทันกาล อันจะช่วยลดโอกาสในการเกิดความเสียหายต่อประชาชนอย่างมีประสิทธิผล โดยต้องดำเนินการอย่างน้อย ดังนี้

(1) จัดให้มีกลไกการแลกเปลี่ยนข้อมูลที่สามารถส่งผ่านข้อมูลได้อย่างถูกต้องและรวดเร็ว โดยกำหนดแนวทาง กระบวนการ และช่องทางการสื่อสารประสานงานในการป้องกัน ติดตามและตรวจจับ จัดการและแก้ไขเหตุภัยทุจริตดิจิทัลระหว่างผู้ให้บริการทางการเงินกับหน่วยงานกำกับดูแลหรือหน่วยงานที่เกี่ยวข้อง เช่น สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานตำรวจแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ ผู้ประกอบกิจการโทรคมนาคม และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ตามที่กำหนดในกฎหมายว่าด้วยมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งมอบหมายฝ่ายงานทำหน้าที่ดูแลและประสานงานร่วมกับหน่วยงานอื่นอย่างชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็ว

<u>ตัวอย่างการดำเนินการเพื่อยกระดับระบบการแลกเปลี่ยนข้อมูล</u>

- ระบบ Central Fraud Registry (CFR) ที่สามารถแลกเปลี่ยนข้อมูลสำคัญได้อย่างถูกต้องครบถ้วนและมีกลไกที่ช่วยให้ดำเนินการได้ทันที (real time) โดยตัวอย่างข้อมูลสำคัญได้แก่ ข้อมูลบัญชีม้าทั้งการแจ้งใหม่และการปลดบัญชี การติดตามเส้นทางเงิน การระงับบัญชี รวมถึงข้อมูลที่จำเป็นต้องใช้ในการประเมินประสิทธิผลและความเหมาะสมของนโยบายทางการ

(2) สนับสนุนข้อมูลที่ต้องใช้ในการสืบสวนสอบสวนและติดตามหาผู้กระทำผิด ให้แก่พนักงานสอบสวนที่ได้รับมอบหมายเมื่อถูกร้องขออย่างทันกาล โดยจัดให้มีผู้รับผิดชอบดูแลและประสานงานอย่างชัดเจน

5.3.4 การสร้างความตระหนักรู้ถึงภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

ผู้ให้บริการทางการเงินมีหน้าที่ในการสร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัลให้แก่ลูกค้าและประชาชน เพื่อป้องกันและลดโอกาสเกิดความเสียหาย ดังนี้

(1) สร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัลในลักษณะเชิงรุกอย่างเป็นวงกว้างและสม่ำเสมอ ด้วยวิธีที่เกิดผลอย่างเป็นรูปธรรมในทางปฏิบัติผ่านช่องทางที่ลูกค้าสามารถเข้าถึงได้ง่าย อย่างน้อยเดือนละ 1 ครั้ง เช่น การแจ้งเตือนผ่านแอปพลิเคชันที่ติดตั้งบนอุปกรณ์เคลื่อนที่ การจัดทำสื่อ infographic บนสื่อทางสังคม รวมทั้งให้การสนับสนุนหน่วยงานอื่นที่เกี่ยวข้องโดยมีเนื้อหาครอบคลุมรูปแบบต่าง ๆ ของภัยทุจริตดิจิทัลที่เกิดขึ้นในปัจจุบัน วิธีการป้องกัน และแนวทางการแจ้งปัญหาเมื่อเกิดเหตุ เพื่อให้ประชาชนโดยเฉพาะลูกค้ากลุ่มเปราะบาง เกิดความเข้าใจและเพิ่มความระมัดระวังในการทำธุรกรรมทางการเงิน

(2) ธนาคารแห่งประเทศไทยสนับสนุนให้ผู้ให้บริการทางการเงินจัดให้มีการประเมินความตระหนักรู้ต่อภัยทุจริต (awareness test) เมื่อลูกค้าเริ่มต้นใช้บริการ mobile banking และบริการเงินอิเล็กทรอนิกส์ที่โอนเงินได้ ครั้งแรก และประเมินอย่างต่อเนื่องทุก ๆ 6 เดือน เป็นขั้นต่ำ เพื่อสร้างความตระหนักรู้ต่อภัยทุจริตดิจิทัล และเพิ่มภูมิคุ้มกันต่อรูปแบบการหลอกลวงใหม่ ๆ โดยอาจพิจารณานำผลการประเมินไปใช้ประกอบกระบวนการป้องกันภัยทุจริตอื่นให้มีประสิทธิภาพยิ่งขึ้น เช่น ใช้เป็นปัจจัยเพิ่มเติมในการกำหนดระดับความเสี่ยงของลูกค้า การกำหนดความเข้มข้นในการสร้างความตระหนักรู้ หรือกำหนดค่าเริ่มต้นของวงเงินการทำธุรกรรมต่อวัน

5.3.5 การรายงานข้อมูลต่อธนาคารแห่งประเทศไทย

ผู้ให้บริการทางการเงินต้องจัดทำและจัดส่งแบบรายงานในรูปแบบและตามระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนด รวมถึงจัดทำและจัดส่งรายงานและข้อมูลอื่นเพิ่มเติมเป็นรายกรณีตามที่ธนาคารแห่งประเทศไทยร้องขอ

5.3.6 การเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษ

กรณีที่ผู้ให้บริการทางการเงินถูกเปรียบเทียบปรับหรือถูกกล่าวโทษอันเนื่องมาจากการปฏิบัติฝ่าฝืนหรือไม่ปฏิบัติตามประกาศฉบับนี้ ให้ผู้ให้บริการทางการเงินเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษดังกล่าวตามหลักเกณฑ์การเปิดเผยข้อมูลที่กำหนดในประกาศธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct) หรือหลักเกณฑ์อื่นที่เกี่ยวข้อง โดยอนุโลม

อย่างไรก็ดี ธนาคารแห่งประเทศไทยขอสงวนสิทธิในการไม่ให้ผู้ให้บริการทางการเงิน เปิดเผยข้อมูลการถูกดำเนินการทางกฎหมายตามที่ระบุข้างต้น หากเห็นว่าอาจกระทบกับความปลอดภัยหรือความผาสุกของประชาชน รวมถึงประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัล

6. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ 1 เมษายน 2568 เป็นต้นไป

ประกาศ ณ วันที่ มีนาคม 2568

(นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

งานจัดการภัยทุจริตทางการเงิน
โทรศัพท์ 0 2283 6685, 0 2283 5834
อีเมล antifraud-policy@bot.or.th