ธนาคารแห่งประเทศไทย

17 ธันวาคม 2568

เรียน ผู้จัดการ

สถาบันการเงินทุกแห่ง
ผู้ประกอบธุรกิจระบบโอนเงินรายย่อยระหว่างผู้ใช้บริการของระบบ
ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ที่มิใช่สถาบันการเงิน
ผู้ประกอบธุรกิจบริการโอนเงินด้วยวิธีการทางอิเล็กทรอนิกส์ที่มิใช่สถาบันการเงิน

ที่ ธปท.ว. 8204 /2568 เรื่อง นำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management)

ธนาคารแห่งประเทศไทยขอนำส่งประกาศธนาคารแห่งประเทศไทย ที่ 57/2568 เรื่อง หลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management) ลงวันที่ 4 ธันวาคม 2568 ซึ่งได้ประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 142 ตอนพิเศษ 392 ง ลงวันที่ 16 ธันวาคม 2568 และมีผลบังคับใช้ตั้งแต่วันที่ 17 ธันวาคม 2568 เป็นต้นไป

การออกประกาศในครั้งนี้มีวัตถุประสงค์ให้ผู้ให้บริการทางการเงินยกระดับการบริหารจัดการภัยทุจริตดิจิทัลตั้งแต่ต้นจนจบกระบวนการ (end-to-end) เพื่อให้การบริหารจัดการภัยทุจริตดิจิทัลเป็นไปอย่างมีประสิทธิผล ช่วยป้องกันและลดความเสียหายที่จะเกิดขึ้นกับประชาชน และรักษาความเชื่อมั่นในระบบสถาบันการเงินและระบบการชำระเงินของประเทศ

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นางสาวดารณี แซ่จู)
ผู้ช่วยผู้ว่าการ สายกำกับระบบการชำระเงิน
และคุ้มครองผู้ใช้บริการทางการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย ประกาศธนาคารแห่งประเทศไทย ที่ 57/2568 เรื่อง หลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management)

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

ธนาคารแห่งประเทศไทย

ประกาศธนาคารแห่งประเทศไทย

ที่ 57 / 2568

เรื่อง หลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management)

---

1. เหตุผลในการออกประกาศ

เนื่องจากภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงินมีหลากหลายรูปแบบ ไม่ว่าจะเป็นการสวมรอยทำธุรกรรมแทนลูกค้า (unauthorized payment fraud) หรือการหลอกลวงหรือข่มขู่ลูกค้าให้โอนเงินแก่มิจฉาชีพด้วยตนเอง (authorized payment fraud) ก่อให้เกิดความเสียหายต่อประชาชนในวงกว้างและกระทบต่อระบบเศรษฐกิจโดยรวม ซึ่งธนาคารแห่งประเทศไทยตระหนักถึงความสำคัญในการบริหารจัดการภัยทุจริตดิจิทัลดังกล่าว จึงได้ออกหลักเกณฑ์และมาตรการต่าง ๆ ให้ผู้ให้บริการทางการเงินถือปฏิบัติมาอย่างต่อเนื่อง ประกอบด้วยการออกหลักเกณฑ์ว่าด้วยมาตรฐานและมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีสำหรับสถาบันการเงิน ตามอำนาจหน้าที่ที่กำหนดในพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และการออกหลักเกณฑ์เพื่อยกระดับการกำกับดูแลของธนาคารแห่งประเทศไทยในการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ เพื่อเป็นการป้องกันประชาชนจากการตกเป็นเหยื่อของมิจฉาชีพในรูปแบบ unauthorized payment fraud อย่างไรก็ตาม ปัจจุบันมิจฉาชีพมีรูปแบบวิธีการ และเทคนิคที่หลากหลายมากยิ่งขึ้น โดยเฉพาะรูปแบบ authorized payment fraud ที่ยังคงเป็นปัญหาสำคัญของประเทศไทย โดยมิจฉาชีพมีการใช้บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ของตนเองหรือผู้อื่นเป็นเครื่องมือในการรับเงินและถ่ายโอนเงินที่ได้จากการกระทำความผิด ส่งผลให้ประชาชนจำนวนมากได้รับความเดือดร้อนต้องสูญเสียเงินจำนวนมากให้กับมิจฉาชีพ

ในครั้งนี้ ธนาคารแห่งประเทศไทยได้ออกประกาศหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management) เพื่อยกระดับการปฏิบัติตามแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน และหนังสือเวียน เรื่อง การเพิ่มความเข้มงวดในการจัดการบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ในกรณีลูกค้ามีความเสี่ยงสูงหรือใช้บัญชีที่มีลักษณะหรือพฤติกรรมผิดปกติ ให้มีความครอบคลุมและมีประสิทธิผลมากขึ้น โดยให้ผู้ให้บริการทางการเงินถือปฏิบัติในการบริหารจัดการภัยทุจริตดิจิทัลตั้งแต่ต้นจนจบกระบวนการ (end-to-end) เริ่มตั้งแต่การป้องกัน ติดตามและตรวจจับ จัดการและแก้ไขเมื่อเกิดเหตุภัยทุจริตดิจิทัล รวมทั้งดูแลลูกค้าที่ได้รับผลกระทบจากภัยทุจริตดิจิทัลดังกล่าว เพื่อให้การบริหารจัดการภัยทุจริตดิจิทัลเป็นไปอย่างมีประสิทธิผล สอดรับกับสภาพแวดล้อมทางการเงินที่เปลี่ยนแปลงไป ช่วยป้องกันและลดความเสียหายที่จะเกิดขึ้นกับประชาชนและรักษาความเชื่อมั่นในระบบสถาบันการเงินและระบบการชำระเงินของประเทศ

2. อำนาจตามกฎหมาย

2.1 อาศัยอำนาจตามความในมาตรา 39 มาตรา 41 มาตรา 57 มาตรา 71 และมาตรา 84 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัลให้สถาบันการเงินและบริษัทในกลุ่มธุรกิจทางการเงินของสถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

2.2 อาศัยอำนาจตามความในมาตรา 24 และมาตรา 26 แห่งพระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัลให้ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ ได้แก่ ผู้ประกอบธุรกิจระบบโอนเงินรายย่อยระหว่างผู้ใช้บริการของระบบ ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ และผู้ประกอบธุรกิจบริการโอนเงินด้วยวิธีการทางอิเล็กทรอนิกส์ถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

3. แนวนโยบายและหนังสือเวียนที่ยกเลิก

3.1 แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ลงวันที่ 29 มีนาคม 2566 เฉพาะส่วนที่เกี่ยวข้องกับผู้ให้บริการทางการเงินตามประกาศฉบับนี้

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

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ให้บริการทางการเงิน ดังต่อไปนี้

4.1 สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

4.2 บริษัทในกลุ่มธุรกิจทางการเงินของสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินที่ประกอบธุรกิจธนาคารพาณิชย์และธุรกิจบริการเงินอิเล็กทรอนิกส์ในต่างประเทศ

4.3 ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน ได้แก่ ผู้ประกอบธุรกิจระบบโอนเงินรายย่อยระหว่างผู้ใช้บริการของระบบ ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ และผู้ประกอบธุรกิจบริการโอนเงินด้วยวิธีการทางอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยระบบการชำระเงิน

5. เนื้อหา

5.1 คำจำกัดความ

ในประกาศฉบับนี้

“ภัยทุจริตดิจิทัล (Digital Fraud)” หมายความว่า ภัยจากการทำธุรกรรมทางการเงินที่เกิดจากการกระทำความผิดหรือพยายามกระทำความผิดผ่านช่องทางดิจิทัลโดยทุจริต

“ผู้ให้บริการทางการเงิน” หมายความว่า สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน บริษัทในกลุ่มธุรกิจทางการเงินของสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ที่ประกอบธุรกิจธนาคารพาณิชย์และธุรกิจบริการเงินอิเล็กทรอนิกส์ในต่างประเทศ ผู้ประกอบธุรกิจระบบโอนเงินรายย่อยระหว่างผู้ใช้บริการของระบบ ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ และผู้ประกอบธุรกิจบริการโอนเงินด้วยวิธีการทางอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยระบบการชำระเงิน

“สถาบันการเงินเฉพาะกิจ” หมายความว่า สถาบันการเงินของรัฐที่มีกฎหมายเฉพาะจัดตั้งขึ้น ได้แก่ ธนาคารออมสิน ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ธนาคารอาคารสงเคราะห์ ธนาคารอิสลามแห่งประเทศไทย ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย และธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

“ลูกค้า” หมายความว่า บุคคลธรรมดา นิติบุคคล หรือบุคคลที่มีการตกลงกันทางกฎหมาย ซึ่งสร้างความสัมพันธ์ทางธุรกิจหรือทำธุรกรรมกับผู้ให้บริการทางการเงิน

“บัญชี” หมายความว่า บัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์

“การทำธุรกรรมทางการเงิน” หมายความว่า การทำธุรกรรมทางการเงินที่ผู้ให้บริการทางการเงินให้บริการ เช่น การเปิดบัญชี การสมัครใช้บริการ การฝากเงิน การถอนเงิน การโอนเงิน การชำระค่าสินค้าและบริการ โดยผ่านช่องทางการให้บริการต่าง ๆ เช่น สาขาทั่วไป สาขาอิเล็กทรอนิกส์ ช่องทางดิจิทัล ทั้งนี้ ไม่รวมถึงการทำธุรกรรมทางการเงินผ่านบัตรเครดิต บัตรเดบิต และบัตรเอทีเอ็ม

“บัญชีม้า” หมายความว่า บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ ซึ่งถูกนำมาใช้หรืออาจถูกนำมาใช้เป็นเครื่องมือในการรับเงินและถ่ายโอนเงินที่ได้มาจากอาชญากรรมทางเทคโนโลยี

“มาตรฐานอุตสาหกรรม (industry standards)” หมายความว่า มาตรฐานอุตสาหกรรมที่ผู้ให้บริการทางการเงินในแต่ละประเภทธุรกิจได้ร่วมกันจัดทำเพื่อเป็นแนวปฏิบัติในการบริหารจัดการภัยทุจริตดิจิทัลของแต่ละประเภทธุรกิจ

5.2 หลักการ

ผู้ให้บริการทางการเงินต้องมีการบริหารจัดการภัยทุจริตดิจิทัลอย่างเหมาะสม และทันกาลกับรูปแบบ วิธีการ และเทคนิคการทุจริตที่มีการเปลี่ยนแปลงไป โดยดำเนินการในแนวทางที่เป็นประโยชน์ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และเป็นการป้องกันและลดความเสียหายที่จะเกิดขึ้นกับประชาชนอย่างมีประสิทธิผล โดยต้องพิจารณาให้เกิดความสมดุลระหว่างความสะดวกและความปลอดภัยในการทำธุรกรรมทางการเงิน และคำนึงถึงการคุ้มครองลูกค้าอย่างเป็นธรรมด้วย

5.3 หลักเกณฑ์

5.3.1 การกำหนดนโยบายและการกำกับดูแลการบริหารจัดการภัยทุจริตดิจิทัล

คณะกรรมการของผู้ให้บริการทางการเงินและผู้บริหารในตำแหน่งสูงสุดของผู้ให้บริการทางการเงินต้องกำกับดูแลให้ผู้ให้บริการทางการเงินมีการบริหารจัดการภัยทุจริตดิจิทัลที่เหมาะสมกับรูปแบบ วิธีการ เทคนิคการทุจริตและผลกระทบของภัยทุจริตดิจิทัลที่เกิดขึ้น และมีการแก้ไขสถานการณ์ที่ทันกาล เพื่อป้องกันและลดความเสียหายที่จะเกิดขึ้นกับลูกค้า ตั้งแต่ต้นจนจบกระบวนการ (end-to-end) โดยเริ่มตั้งแต่การป้องกัน ติดตามและตรวจจับ จัดการและแก้ไขเมื่อเกิดเหตุภัยทุจริตดิจิทัล รวมทั้งดูแลลูกค้าที่ได้รับผลกระทบจากภัยทุจริตดังกล่าว โดยกำหนดให้เป็นความเสี่ยงสำคัญที่องค์กรต้องมีการบริหารจัดการร่วมกันแบบบูรณาการ โดยผู้ให้บริการทางการเงินต้องดำเนินการ ดังนี้

(1) กำหนดให้มีคณะทำงานหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทำหน้าที่กำหนดนโยบายและกำกับดูแลการบริหารจัดการภัยทุจริตดิจิทัล เพื่อให้องค์กรให้ความสำคัญและมีแนวทางบริหารจัดการภัยทุจริตดิจิทัลที่เหมาะสม ทันกาล และมีประสิทธิผลอย่างต่อเนื่อง สอดรับกับบริบทของปัญหาภัยทุจริตในแต่ละช่วงเวลา และสามารถลดความเสียหายที่จะเกิดขึ้นกับลูกค้าได้ทันท่วงที

(2) กำหนดนโยบายการบริหารจัดการภัยทุจริตดิจิทัลที่ชัดเจน เป็นลายลักษณ์อักษร โดยได้รับความเห็นชอบจากคณะกรรมการของผู้ให้บริการทางการเงิน และนโยบายดังกล่าวต้องสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง บริบทของปัญหาภัยทุจริตดิจิทัลในแต่ละช่วงเวลา และครอบคลุมอย่างน้อย ดังนี้

(2.1) บทบาทหน้าที่ของคณะทำงาน หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย และหน่วยงานที่รับผิดชอบ เพื่อผลักดันให้มีการบริหารจัดการภัยทุจริตดิจิทัลที่มีประสิทธิผล โดยครอบคลุมตั้งแต่ต้นจนจบกระบวนการ (end-to-end) รวมทั้งประเมินความพร้อมขององค์กรทั้งในด้านบุคลากร กระบวนการ เทคโนโลยีและเครื่องมือที่ใช้ในการจัดการภัยทุจริตดิจิทัลอย่างสม่ำเสมอ

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

(2.3) การติดตามและวัดประสิทธิผลของการจัดการภัยทุจริตดิจิทัลอย่างต่อเนื่อง เพื่อทบทวนและปรับปรุงแนวทางและกระบวนการบริหารจัดการภัยทุจริตดิจิทัลให้เหมาะสมกับสถานการณ์อยู่เสมอ

ทั้งนี้ ผู้ให้บริการทางการเงินต้องจัดให้มีการทบทวนและปรับปรุงนโยบายการบริหารจัดการภัยทุจริตดิจิทัลอย่างสม่ำเสมอ โดยเฉพาะเมื่อมีเหตุการณ์หรือการเปลี่ยนแปลงที่ส่งผลกระทบต่อประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัลอย่างมีนัยสำคัญหรือตามความถี่ที่เหมาะสม ทั้งนี้ หากเป็นการปรับปรุงที่มีนัยสำคัญ ต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ให้บริการทางการเงิน และหากเป็นการปรับปรุงที่ไม่มีนัยสำคัญ คณะทำงานหรือผู้บริหารระดับสูงที่ได้รับมอบหมายสามารถดำเนินการได้โดยต้องรายงานคณะกรรมการของผู้ให้บริการทางการเงินเพื่อทราบในภายหลังด้วย

(3) จัดให้มีบุคลากร กระบวนการ เทคโนโลยีและเครื่องมือที่ใช้ในการจัดการภัยทุจริตดิจิทัลอย่างเพียงพอและเหมาะสม โดยในการออกแบบและพัฒนาระบบงาน กระบวนการและผลิตภัณฑ์หรือบริการทางการเงิน ต้องคำนึงถึงเหตุการณ์และปัจจัยความเสี่ยงที่อาจทำให้เกิดภัยทุจริตดิจิทัล เช่น การยกระดับกระบวนการรู้จักลูกค้าเพื่อป้องกันการสวมรอยสมัครใช้บริการทางการเงินแทนลูกค้าตัวจริง การยกระดับการยืนยันตัวตนเพื่อป้องกันการถูกผู้ไม่ประสงค์ดีทำธุรกรรมทางการเงินโดยไม่ได้รับอนุญาตแทนลูกค้าตัวจริง การกำหนดเพดานวงเงินการทำธุรกรรมเพื่อป้องกันและลดความเสียหายที่จะเกิดขึ้นกับลูกค้า

(4) จัดให้มีการสื่อสารเผยแพร่นโยบายและแนวทางการบริหารจัดการภัยทุจริตดิจิทัลให้ทุกฝ่ายงานที่เกี่ยวข้องในองค์กรนำไปปฏิบัติได้อย่างเหมาะสม รวมทั้งพัฒนาองค์ความรู้ของบุคลากรในองค์กรเกี่ยวกับการบริหารจัดการภัยทุจริตดิจิทัลอย่างต่อเนื่อง เพื่อให้พนักงานที่เกี่ยวข้องทุกระดับมีความรู้ความเข้าใจที่เพียงพอในการกำกับดูแลและการบริหารจัดการภัยทุจริตดิจิทัลรูปแบบใหม่ ๆ ที่อาจเกิดขึ้น

(5) จัดให้หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง หน่วยงานที่ทำหน้าที่กำกับการปฏิบัติตามกฎเกณฑ์ และหน่วยงานที่ทำหน้าที่ตรวจสอบภายใน ต้องมีส่วนร่วมในการผลักดันให้องค์กรมีกระบวนการควบคุมดูแลความเสี่ยงที่ดี เพื่อให้การบริหารจัดการภัยทุจริตดิจิทัลขององค์กรดำเนินการได้อย่างเหมาะสม และทันกาล

(6) กำหนดเป้าหมายและตัวชี้วัดในการประเมินประสิทธิผลของการจัดการภัยทุจริตดิจิทัลที่ชัดเจนและวัดผลได้จริง ครอบคลุมตั้งแต่ต้นจนจบกระบวนการ (end-to-end) และต้องปรับปรุงเป้าหมายและตัวชี้วัดดังกล่าวอย่างสม่ำเสมอเพื่อให้สอดคล้องกับรูปแบบ วิธีการและเทคนิคการทุจริตของภัยทุจริตดิจิทัลที่เปลี่ยนแปลงไป

(7) ติดตามและประเมินประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัล รวมทั้งปรับปรุงระบบงาน กระบวนการ และผลิตภัณฑ์หรือบริการทางการเงิน ให้ครอบคลุมรูปแบบ วิธีการ และเทคนิคการทุจริตของภัยทุจริตดิจิทัลที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง เพื่อให้สามารถตรวจจับและจัดการธุรกรรมที่มีความผิดปกติได้ทันท่วงที โดยผู้บริหารในตำแหน่งสูงสุด คณะทำงาน หรือผู้บริหารระดับสูงที่ได้รับมอบหมายต้องจัดให้มีการรายงานประเด็นที่มีนัยสำคัญต่อคณะกรรมการของผู้ให้บริการทางการเงินอย่างสม่ำเสมอ

(8) สนับสนุนการจัดทำมาตรฐานอุตสาหกรรม (industry standards) โดยให้ครอบคลุมกระบวนการบริหารจัดการภัยทุจริตดิจิทัลที่จำเป็นและสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง เพื่อให้มั่นใจว่ากระบวนการบริหารจัดการภัยทุจริตดิจิทัลมีมาตรฐานเดียวกัน

5.3.2 กระบวนการจัดการภัยทุจริตดิจิทัล

ผู้ให้บริการทางการเงินต้องจัดให้มีกรอบการดำเนินการบริหารจัดการภัยทุจริตดิจิทัลที่ชัดเจนตลอดวงจรการใช้บริการของลูกค้า เริ่มตั้งแต่ลูกค้าสมัครใช้บริการหรือเปิดบัญชี ทำธุรกรรมทางการเงิน จนถึงปิดบัญชี ยกเลิกการใช้บริการ หรือยุติความสัมพันธ์ โดยต้องครอบคลุมกระบวนการอย่างน้อย ดังนี้

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

ผู้ให้บริการทางการเงินต้องดำเนินการตามกระบวนการรู้จักลูกค้า (Know Your Customer: KYC) โดยระบุและพิสูจน์ทราบตัวตนของลูกค้าจากแหล่งข้อมูลที่น่าเชื่อถือ เพื่อให้มั่นใจว่าข้อมูลที่ได้รับจากลูกค้าเป็นข้อมูลที่แท้จริง มีความถูกต้อง และเป็นปัจจุบัน รวมถึงต้องสอบถามวัตถุประสงค์ในการเปิดบัญชีของลูกค้า และวิเคราะห์ลักษณะหรือพฤติการณ์ของลูกค้าร่วมด้วย และต้องดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าเมื่อเริ่มทำธุรกรรมครั้งแรกและตรวจสอบเป็นระยะจนสิ้นสุดเมื่อมีการปิดบัญชีหรือยุติความสัมพันธ์กับลูกค้าตามหลักเกณฑ์ของกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน โดยหากผู้ให้บริการทางการเงินพบว่าลูกค้ามีความเสี่ยงต่อการนำบัญชีไปใช้เป็นบัญชีม้า เช่น มีพฤติกรรมการใช้บัญชีที่ไม่สอดคล้องกับข้อมูลของลูกค้า หรืออยู่ในรายชื่อบุคคลที่มีความเสี่ยงที่ได้รับจากฐานข้อมูลที่น่าเชื่อถือ ผู้ให้บริการทางการเงินต้องยกระดับการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าให้อยู่ในระดับที่เข้มข้น (Enhanced Customer Due Diligence: EDD) โดยตรวจสอบข้อมูลอื่นเพิ่มเติม เช่น แหล่งที่มาของเงินหรือทรัพย์สิน แหล่งที่มาของฐานะความมั่งคั่ง รวมถึงข้อมูลเกี่ยวกับการประกอบกิจการของลูกค้า อาชีพ ชื่อและสถานที่ตั้งของที่ทำงาน

ทั้งนี้ ผู้ให้บริการทางการเงินต้องนำข้อมูลที่ได้จากการรู้จักลูกค้า การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า และจากฐานข้อมูลที่น่าเชื่อถือ มาประเมินและจัดกลุ่มลูกค้าตามระดับความเสี่ยงที่ลูกค้าอาจนำบัญชีไปใช้เป็นบัญชีม้าหรืออาจถูกหลอกลวงจนเกิดความเสียหาย รวมทั้งทบทวนระดับความเสี่ยงของลูกค้าให้เป็นปัจจุบันและเหมาะสมกับบริบทที่เปลี่ยนแปลงไปอยู่เสมอ

(2) การติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงิน (monitoring and detection)

ผู้ให้บริการทางการเงินต้องมีกระบวนการติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงินในเชิงรุกอย่างมีประสิทธิผล ครอบคลุมรูปแบบของภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงินที่เปลี่ยนแปลงไปอย่างต่อเนื่อง โดยต้องสามารถประเมินระดับความเสี่ยงของบัญชี ทั้งบัญชีของบุคคลที่คาดว่าจะได้รับความเสียหายจากภัยทุจริตดิจิทัลและบุคคลที่มีความเสี่ยงในการนำบัญชีไปใช้เป็นบัญชีม้า รวมถึงตรวจจับการทำธุรกรรมและการใช้บัญชีที่มีความผิดปกติได้อย่างทันท่วงที เพื่อให้มีการจัดการภัยทุจริตดิจิทัลที่เหมาะสมและทันกาล ซึ่งจะมีส่วนทำให้สามารถป้องกันและจำกัดความเสียหายที่เกิดจากภัยทุจริตดิจิทัลไม่ให้ขยายตัวหรือลุกลามเป็นวงกว้าง ดังนี้

(2.1) จัดให้มีระบบการติดตามและตรวจจับธุรกรรมที่ผิดปกติได้ทันท่วงที โดยต้องกำหนดเงื่อนไขในการติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงิน ทั้งธุรกรรมของบุคคลที่คาดว่าจะได้รับความเสียหายจากภัยทุจริตดิจิทัลและบุคคลที่มีความเสี่ยงในการนำบัญชีไปใช้เป็นบัญชีม้า โดยต้องพิจารณาถึงรูปแบบของภัยทุจริตดิจิทัลที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง ทั้งที่เกิดขึ้นภายในประเทศไทยและในต่างประเทศ ช่องทางการให้บริการ พฤติกรรมการใช้บัญชี ข้อมูลพฤติกรรมต้องสงสัยที่ผู้ให้บริการทางการเงินตรวจพบเอง ข้อมูลที่ได้รับจากผู้ให้บริการทางการเงินแห่งอื่น ข้อมูลจากระบบ Central Fraud Registry (CFR) และข้อมูลจากหน่วยงานอื่น ๆ

(2.2) ทบทวนและปรับปรุงเงื่อนไข รวมทั้งกระบวนการในการตรวจจับความผิดปกติในการทำธุรกรรมทางการเงินในเชิงรุก (proactive detection) อย่างสม่ำเสมอ โดยนำระบบวิเคราะห์ข้อมูล (data analytics) หรือเทคโนโลยีปัญญาประดิษฐ์ (artificial intelligence) มาใช้เพื่อให้สามารถติดตามและตรวจจับความผิดปกติได้ดียิ่งขึ้น และเท่าทันกับสถานการณ์และรูปแบบภัยทุจริตดิจิทัลใหม่ ๆ อันจะช่วยให้ผู้ให้บริการทางการเงินสามารถระงับเหตุการณ์ภัยทุจริตดิจิทัลและป้องกันหรือจำกัดความเสียหายที่อาจเกิดขึ้นได้อย่างทันกาล

(3) การจัดการภัยทุจริตดิจิทัล (actions)

ผู้ให้บริการทางการเงินต้องมีการป้องกัน จำกัด และระงับความเสียหายจากภัยทุจริตดิจิทัลอย่างรวดเร็ว เพียงพอและเหมาะสม สอดคล้องตามระดับความเสี่ยงของธุรกรรมทางการเงิน ซึ่งประกอบด้วยการป้องกันและจำกัดความเสียหายให้แก่ลูกค้า และการจัดการบัญชีที่อาจเข้าข่ายเป็นบัญชีม้าเพื่อจำกัดและระงับความเสียหาย โดยต้องจัดให้มีการจัดการอย่างน้อย ดังนี้

(3.1) การป้องกันและจำกัดความเสียหายให้แก่ลูกค้า

ผู้ให้บริการทางการเงินต้องจัดให้มีการป้องกันและจำกัดความเสียหายแก่ลูกค้าอย่างเพียงพอและเหมาะสมตามระดับความเสี่ยงของการทำธุรกรรมทางการเงิน เช่น มีกระบวนการยืนยันตัวตนลูกค้า (authentication) ที่รัดกุมและเหมาะสมกับความเสี่ยงของลูกค้า

ธุรกรรม ผลิตภัณฑ์และบริการ และช่องทางการให้บริการ การแจ้งเตือน หน่วง หรือระงับการทำธุรกรรมที่มีความผิดปกติตามระดับความเสี่ยงของธุรกรรม รวมถึงการกำหนดวงเงินการทำธุรกรรมของลูกค้าให้เหมาะสมกับระดับความเสี่ยงและสอดคล้องกับการใช้งานตามปกติของลูกค้า เพื่อลดความเสียหายจากภัยทุจริตดิจิทัล

(3.2) การจัดการบัญชีที่อาจเข้าข่ายเป็นบัญชีม้าเพื่อจำกัดและระงับความเสียหาย

ผู้ให้บริการทางการเงินต้องจัดให้มีการจำกัดและระงับความเสียหายและผลกระทบของความเสียหายให้สอดคล้องกับระดับความเสี่ยงของบุคคลที่นำบัญชีไปใช้เป็นบัญชีม้าหรืออาจนำบัญชีไปใช้เป็นบัญชีม้าได้อย่างเหมาะสมและทันกาล เช่น การระงับเงินเข้า การระงับเงินออก การระงับการให้บริการผ่านช่องทางอิเล็กทรอนิกส์ การปฏิเสธการเปิดบัญชีใหม่ การควบคุมการถอนเงินสด

(4) การแก้ไขสถานการณ์และการดูแลลูกค้า (response)

ผู้ให้บริการทางการเงินต้องแก้ไขสถานการณ์และดูแลลูกค้าเมื่อเกิดเหตุการณ์ภัยทุจริตดิจิทัลอย่างชัดเจน รวดเร็ว และเป็นธรรม โดยขั้นต่ำต้องดำเนินการ ดังนี้

(4.1) การจัดให้มีช่องทางรับแจ้งเหตุการณ์ต้องสงสัยหรือเหตุการณ์ภัยทุจริตดิจิทัล

ผู้ให้บริการทางการเงินต้องจัดให้มีช่องทางติดต่อเร่งด่วน (hotline) ทางโทรศัพท์ หรือทางอิเล็กทรอนิกส์เพื่อให้ลูกค้าสามารถติดต่อผู้ให้บริการทางการเงินได้ โดยช่องทางดังกล่าวจะต้องเพียงพอและให้บริการอย่างต่อเนื่องทั้งในและนอกเวลาทำการ (24x7) เพื่อให้ลูกค้าสามารถแจ้งเหตุการณ์ต้องสงสัยหรือเหตุการณ์ที่เป็นภัยทุจริตดิจิทัลได้โดยสะดวกและรวดเร็ว ทั้งนี้ หลังได้รับแจ้งเหตุดังกล่าว ผู้ให้บริการทางการเงินต้องเร่งดำเนินการตามกฎหมายและหลักเกณฑ์อื่นที่เกี่ยวข้องอย่างเคร่งครัด เพื่อให้การติดตามตรวจสอบเหตุการณ์เป็นไปอย่างทันกาล และ จำกัดความเสียหายที่อาจเกิดขึ้น

(4.2) การกำหนดระยะเวลาของกระบวนการดูแลลูกค้า

ผู้ให้บริการทางการเงินต้องกำหนดระยะเวลาของกระบวนการดูแลลูกค้าที่ได้รับความเสียหายที่เกิดขึ้นจากภัยทุจริตดิจิทัลให้ชัดเจน เช่น การแจ้งให้ลูกค้าที่เกี่ยวข้องทราบเมื่อเกิดเหตุการณ์ การติดต่อกลับไปยังลูกค้าดังกล่าวอย่างรวดเร็วภายในเวลาที่เหมาะสมภายหลังลูกค้าแจ้งผู้ให้บริการทางการเงินเกี่ยวกับเหตุการณ์ที่อาจเข้าข่ายเป็นภัยทุจริตดิจิทัล ทั้งนี้ กระบวนการดูแลลูกค้ารวมถึงกระบวนการสื่อสารและการทำความเข้าใจกับลูกค้าเกี่ยวกับปัญหาและผลกระทบที่เกิดขึ้นอย่างทันกาล

(4.3) การดูแลลูกค้า

ผู้ให้บริการทางการเงินต้องดูแลลูกค้าที่ได้รับความเสียหายจากภัยทุจริตดิจิทัลอย่างเหมาะสม รวดเร็ว และเป็นธรรม โดยผู้ให้บริการทางการเงินต้องจัดให้มีผู้รับผิดชอบดูแลและประสานงานอย่างชัดเจน นอกจากนี้ หากการจัดการภัยทุจริตดิจิทัลของผู้ให้บริการทางการเงินก่อให้เกิดผลกระทบต่อลูกค้าที่ไม่มีส่วนเกี่ยวข้องกับการกระทำทุจริต ผู้ให้บริการทางการเงินต้องแก้ไขปัญหาที่เกิดจากผลกระทบดังกล่าวที่รวดเร็ว เช่น การปลดการระงับบัญชีโดยเร็วภายหลังจากที่ได้รับคำสั่งจากหน่วยงานทางการหรือเมื่อได้ดำเนินการพิจารณาตามกระบวนการหรือหลักเกณฑ์ของผู้ให้บริการทางการเงินแล้ว การเยียวยาความเสียหายให้แก่ลูกค้าอย่างรวดเร็วเมื่อพิสูจน์ได้ว่าลูกค้าได้รับความเสียหายจากความบกพร่องของผู้ให้บริการทางการเงิน หรือเมื่อได้รับคำสั่งจากหน่วยงานที่เกี่ยวข้อง

(4.4) การรายงานเหตุการณ์ภัยทุจริตดิจิทัล และการสื่อสารต่อสาธารณชน

ผู้ให้บริการทางการเงินต้องรายงานเหตุการณ์ภัยทุจริตดิจิทัลแก่คณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย ให้เหมาะสมตามระดับความรุนแรงของเหตุการณ์ ทั้งนี้ กรณีที่เกิดความเสียหายกับลูกค้าในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของผู้ให้บริการทางการเงิน ผู้ให้บริการทางการเงินต้องรายงานเหตุการณ์ภัยทุจริตดิจิทัลให้ธนาคารแห่งประเทศไทยทราบโดยเร็วตามช่องทางที่กำหนด

นอกจากนี้ ในกรณีที่เกิดเหตุการณ์ภัยทุจริตดิจิทัลกับลูกค้าของผู้ให้บริการทางการเงินหรือสถาบันการเงินเฉพาะกิจหรือผู้ประกอบธุรกิจอื่นหลายแห่งพร้อมกันและส่งผลกระทบในวงกว้างต่อความเชื่อมั่นของระบบการเงินหรือระบบการชำระเงิน ผู้ให้บริการทางการเงินที่ลูกค้าของตนได้รับผลกระทบจากภัยทุจริตดิจิทัลดังกล่าวควรร่วมกับผู้ให้บริการทางการเงินอื่น สถาบันการเงินเฉพาะกิจ สมาคมของผู้ให้บริการทางการเงิน สมาคมของสถาบันการเงินเฉพาะกิจ และหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับเหตุการณ์ดังกล่าว จัดให้มีการสื่อสารเพื่อชี้แจงและทำความเข้าใจกับลูกค้าโดยเร็ว และกำหนดแนวทางช่วยเหลือและดูแลลูกค้าให้เป็นมาตรฐานเดียวกัน

5.3.3 การแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับภัยทุจริตดิจิทัล

ผู้ให้บริการทางการเงินต้องจัดให้มีกลไกการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับภัยทุจริตดิจิทัลระหว่างผู้ให้บริการทางการเงิน สถาบันการเงินเฉพาะกิจ และหน่วยงานอื่นที่เกี่ยวข้อง เพื่อให้สามารถร่วมกันบริหารจัดการภัยทุจริตดิจิทัลได้อย่างทันกาล อันจะช่วยลดโอกาสในการเกิดความเสียหายต่อลูกค้าอย่างมีประสิทธิผล โดยต้องดำเนินการอย่างน้อย ดังนี้

(1) จัดให้มีกลไกการแลกเปลี่ยนข้อมูลที่สามารถส่งผ่านข้อมูลได้อย่างถูกต้องและรวดเร็ว เพื่อป้องกัน ติดตามและตรวจจับ จัดการและแก้ไขเหตุภัยทุจริตดิจิทัล โดยต้องเป็นไปตามแนวทางที่กำหนดในกฎหมายว่าด้วยมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี รวมถึงกฎหมายหรือหลักเกณฑ์อื่นที่เกี่ยวข้องด้วย

(2) สนับสนุนข้อมูลที่ต้องใช้ในการสืบสวนสอบสวนและติดตามหาผู้กระทำความผิดให้แก่พนักงานสอบสวนที่ได้รับมอบหมายอย่างทันกาลตามที่พนักงานสอบสวนร้องขอ โดยผู้ให้บริการทางการเงินต้องจัดให้มีผู้รับผิดชอบดูแลและประสานงานอย่างชัดเจน

5.3.4 การสร้างความตระหนักรู้ถึงภัยทุจริตดิจิทัล

ผู้ให้บริการทางการเงินมีหน้าที่ในการสร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัลให้แก่ลูกค้า เพื่อป้องกันและลดโอกาสเกิดความเสียหาย ดังนี้

(1) สร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัลในเชิงรุกให้แก่ลูกค้าในวงกว้างและสม่ำเสมอ ด้วยวิธีที่เกิดผลอย่างเป็นรูปธรรมผ่านช่องทางที่ลูกค้าสามารถเข้าถึงได้ง่าย เช่น การแจ้งเตือนผ่านแอปพลิเคชันที่ติดตั้งบนอุปกรณ์เคลื่อนที่ การจัดทำสื่อ infographic บนสื่อสังคมออนไลน์ โดยมีเนื้อหาครอบคลุมรูปแบบต่าง ๆ ของภัยทุจริตดิจิทัลที่เกิดขึ้นในปัจจุบัน วิธีการป้องกันและแนวทางการแจ้งปัญหาเมื่อเกิดเหตุภัยทุจริตดิจิทัล เพื่อให้ลูกค้าโดยเฉพาะกลุ่มเปราะบางเกิดความเข้าใจและเพิ่มความระมัดระวังในการทำธุรกรรมทางการเงิน รวมทั้งให้การสนับสนุนหน่วยงานอื่นที่เกี่ยวข้องในการสร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัลให้แก่ลูกค้าและประชาชน

(2) ธนาคารแห่งประเทศไทยสนับสนุนให้ผู้ให้บริการทางการเงินจัดให้มีการประเมินความตระหนักรู้ต่อภัยทุจริตดิจิทัล (awareness test) ของลูกค้า โดยรูปแบบของการประเมินต้องคำนึงถึงประสิทธิผลของการสร้างความตระหนักรู้ให้กับลูกค้า และมีการพัฒนารูปแบบของการประเมินอย่างต่อเนื่องให้สอดคล้องกับพฤติกรรมการหลอกลวงของมิจฉาชีพที่เปลี่ยนแปลงไป เพื่อเพิ่มภูมิคุ้มกันของลูกค้าสำหรับรูปแบบภัยทุจริตดิจิทัลต่าง ๆ โดยอาจพิจารณานำผลการประเมินไปใช้ประกอบการจัดทำกระบวนการป้องกันภัยทุจริตดิจิทัลให้มีประสิทธิผลยิ่งขึ้น เช่น ใช้เป็นปัจจัยเพิ่มเติมในการกำหนดระดับความเสี่ยงของลูกค้า การกำหนดความเข้มข้นในการสร้างความตระหนักรู้ หรือกำหนดค่าเริ่มต้นของวงเงินการทำธุรกรรมต่อวัน

5.3.5 การรายงานข้อมูลต่อธนาคารแห่งประเทศไทย

ผู้ให้บริการทางการเงินต้องจัดทำและจัดส่งแบบรายงาน เพื่อประโยชน์ในการติดตามประเมินประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัลในภาพรวมและของผู้ให้บริการทางการเงิน รวมทั้งความเหมาะสมของนโยบายทางการ ตามรูปแบบและระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนด รวมถึงจัดทำและจัดส่งรายงานและข้อมูลอื่นเพิ่มเติมเป็นรายกรณีตามที่ธนาคารแห่งประเทศไทยร้องขอ

5.3.6 การเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษ

กรณีที่ผู้ให้บริการทางการเงิน หรือกรรมการ หรือผู้จัดการ หรือผู้มีอำนาจในการจัดการของผู้ให้บริการทางการเงิน ถูกเปรียบเทียบปรับหรือถูกกล่าวโทษอันเนื่องมาจากการปฏิบัติฝ่าฝืนหรือไม่ปฏิบัติตามประกาศฉบับนี้ ให้ผู้ให้บริการทางการเงินเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษดังกล่าวตามหลักเกณฑ์การเปิดเผยข้อมูลที่กำหนดในประกาศธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct) โดยอนุโลม

อย่างไรก็ดี ในกรณีที่ธนาคารแห่งประเทศไทยเห็นว่าการเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษดังกล่าวอาจกระทบกับความปลอดภัยหรือความผาสุกของประชาชน หรือประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัล ธนาคารแห่งประเทศไทยอาจแจ้งผู้ให้บริการทางการเงินไม่ให้เปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษดังกล่าวก็ได้

ทั้งนี้ ธนาคารแห่งประเทศไทยจะกำหนดแนวปฏิบัติขั้นต่ำสำหรับการบริหารจัดการภัยทุจริตดิจิทัลเพื่อให้ผู้ให้บริการทางการเงินใช้อ้างอิงในการดำเนินการหรือเป็นมาตรฐานขั้นต่ำในการปฏิบัติที่ถือเป็นการปฏิบัติตามหลักเกณฑ์เรื่องใดเรื่องหนึ่งของประกาศฉบับนี้ โดยเมื่อผู้ให้บริการทางการเงินดำเนินการตามแนวปฏิบัติขั้นต่ำดังกล่าวแล้วให้ถือว่าเป็นการปฏิบัติตามหลักเกณฑ์เรื่องนั้น

5.4 การถือปฏิบัติตามหลักเกณฑ์ของผู้ให้บริการทางการเงินแต่ละประเภท

เนื่องจากประกาศฉบับนี้มีขอบเขตใช้บังคับกับผู้ให้บริการทางการเงินหลายประเภท ซึ่งมีลักษณะการประกอบธุรกิจที่มีความเสี่ยงต่อภัยทุจริตดิจิทัลที่แตกต่างกัน ธนาคารแห่งประเทศไทยจึงกำหนดให้ผู้ให้บริการทางการเงินถือปฏิบัติตามหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัลให้เหมาะสมกับลักษณะการประกอบธุรกิจและความเสี่ยงของบริการทางการเงินหรือลักษณะของธุรกรรมของผู้ให้บริการทางการเงินแต่ละประเภท ดังนี้

5.4.1 ผู้ให้บริการทางการเงินประเภทสถาบันการเงินที่เป็นธนาคารพาณิชย์ และผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์เฉพาะรายที่มีบริการโอนเงินไปยังบัญชีของบุคคลอื่นที่มีอยู่กับผู้ให้บริการทางการเงินอื่นได้ ให้ถือปฏิบัติตามหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัลตามข้อ 5.3 ข้างต้นทุกข้อ

5.4.2 ผู้ให้บริการทางการเงินประเภทสถาบันการเงินที่เป็นบริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ที่ไม่มีบริการโอนเงินไปยังบัญชีของบุคคลอื่นที่มีอยู่กับผู้ให้บริการทางการเงินอื่น ผู้ประกอบธุรกิจระบบโอนเงินรายย่อยระหว่างผู้ใช้บริการของระบบ และผู้ประกอบธุรกิจบริการโอนเงินด้วยวิธีการทางอิเล็กทรอนิกส์ ให้นำหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัลตามข้อ 5.3 ข้างต้น ไปปรับใช้ตามระดับความเสี่ยง (risk proportionality) ทั้งในกรณีที่บัญชีของลูกค้าอาจถูกนำไปใช้เป็นบัญชีม้าหรือลูกค้าอาจถูกหลอกลวงจนเกิดความเสียหาย โดยต้องคำนึงถึงขอบเขตการประกอบธุรกิจ กลุ่มลูกค้าที่ให้บริการ ประเภทของผลิตภัณฑ์ ช่องทางการให้บริการ และสภาพแวดล้อมในประเทศและต่างประเทศ โดยถือปฏิบัติอย่างน้อยตามแนวทางการนำหลักเกณฑ์ไปปรับใช้ให้เหมาะสมกับผู้ให้บริการทางการเงินแต่ละประเภท ปรากฏรายละเอียดตามเอกสารแนบท้ายประกาศนี้

5.4.3 สาขาของผู้ให้บริการทางการเงินในต่างประเทศและผู้ให้บริการทางการเงินที่เป็นบริษัทในกลุ่มธุรกิจทางการเงินของสถาบันการเงินที่ประกอบธุรกิจในต่างประเทศ ซึ่งผู้กำกับดูแล

ในต่างประเทศนั้นกำหนดหลักเกณฑ์การกำกับดูแลเกี่ยวกับการบริหารจัดการภัยทุจริตดิจิทัล หรือมีหลักเกณฑ์การกำกับดูแลอื่นใดที่มีข้อกำหนดในลักษณะเดียวกันไว้แล้ว ให้สาขาของผู้ให้บริการทางการเงินในต่างประเทศและผู้ให้บริการทางการเงินที่เป็นบริษัทในกลุ่มธุรกิจทางการเงินของสถาบันการเงินที่ประกอบธุรกิจในต่างประเทศถือปฏิบัติตามหลักเกณฑ์การกำกับดูแลดังกล่าว หรือในกรณีที่ผู้กำกับดูแลในต่างประเทศนั้นไม่มีการกำหนดหลักเกณฑ์การกำกับดูแลเกี่ยวกับการบริหารจัดการภัยทุจริตดิจิทัลไว้ ให้ถือปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ โดยสามารถนำหลักเกณฑ์ในประกาศฉบับนี้ไปปรับใช้ให้เหมาะสมกับกลุ่มลูกค้า ประเภทของผลิตภัณฑ์ ช่องทางการให้บริการ และสภาพแวดล้อมในประเทศนั้น

ทั้งนี้ กรณีผู้ให้บริการทางการเงินมีการให้บริการทางการเงินแก่ลูกค้าที่มีความเสี่ยงต่ำหรือมีการทำธุรกรรมที่มีความเสี่ยงต่ำ ให้ผู้ให้บริการทางการเงินดังกล่าวนำหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัลตามข้อ 5.3 ไปปรับใช้ตามระดับความเสี่ยง (risk proportionality) ของการให้บริการทางการเงินแก่ลูกค้าที่มีความเสี่ยงต่ำ หรือมีการทำธุรกรรมที่มีความเสี่ยงต่ำนั้นได้

6. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป เว้นแต่ข้อ 5.3.1 ให้ใช้บังคับเมื่อพ้นกำหนดเก้าสิบวันนับแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ 4 ธันวาคม 2568

(นายวิทัย รัตนากร)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

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

เอกสารแนบ

แนวทางการพิจารณานำหลักเกณฑ์ไปปรับใช้ให้เหมาะสมกับผู้ให้บริการทางการเงินแต่ละประเภท

หลักเกณฑ์	บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์	ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ที่ไม่มีบริการโอนเงินไปยังบัญชีของบุคคลอื่นที่มีอยู่กับผู้ให้บริการทางการเงินอื่น	ผู้ประกอบธุรกิจบริการโอนเงินด้วยวิธีการทางอิเล็กทรอนิกส์	ผู้ประกอบธุรกิจระบบโอนเงินรายย่อยระหว่างผู้ใช้บริการของระบบ
5.3.1 การกำหนดนโยบายและการกำกับดูแลการบริหารจัดการภัยทุจริตดิจิทัล	✓	✓	✓	✓
5.3.2 กระบวนการจัดการภัยทุจริตดิจิทัล				
(1) กระบวนการรู้จักลูกค้า (KYC) และการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (CDD)	✓	✓	✓	N/A
(2) การติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงิน (monitoring and detection)	จัดให้มีการติดตามและตรวจจับธุรกรรมที่ผิดปกติที่เหมาะสมกับความเสี่ยงและลักษณะการประกอบธุรกิจ			จัดให้มีระบบงาน และเครื่องมือที่ช่วยให้ผู้ใช้บริการของระบบสามารถป้องกันและตรวจจับความเสี่ยงจากภัยทุจริตดิจิทัลได้อย่างมีประสิทธิผลและประสิทธิภาพ รวมถึงสนับสนุนข้อมูลที่เป็นประโยชน์ให้ผู้ใช้บริการพัฒนาระบบติดตามและตรวจจับภัยทุจริตดิจิทัล

หลักเกณฑ์		บริษัทเงินทุน และบริษัท เครดิตฟองซิเอร์	ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์<u>ที่ไม่มี</u> บริการโอนเงินไปยังบัญชีของบุคคลอื่นที่มีอยู่กับผู้ให้บริการทางการเงินอื่น	ผู้ประกอบธุรกิจบริการโอนเงินด้วยวิธีการทางอิเล็กทรอนิกส์	ผู้ประกอบธุรกิจระบบโอนเงินรายย่อยระหว่างผู้ใช้บริการของระบบ
(3) การจัดการภัยทุจริตดิจิทัล (actions)	(3.1) การป้องกันและจำกัดความเสียหายให้แก่ลูกค้า	จัดให้มีการป้องกันและจำกัดความเสียหายให้แก่ลูกค้าที่เหมาะสมเมื่อตรวจพบธุรกรรมที่ผิดปกติ			N/A
	(3.2) การจัดการบัญชีที่อาจเข้าข่ายเป็นบัญชีม้าเพื่อจำกัดและระงับความเสียหาย	✓	✓	✓	N/A
(4) การแก้ไขสถานการณ์และการดูแลลูกค้า (response)	(4.1) การจัดให้มีช่องทางรับแจ้งเหตุการณ์ต้องสงสัยหรือเหตุการณ์ภัยทุจริตดิจิทัล	จัดให้มีช่องทางการติดต่อเร่งด่วนที่ลูกค้าสามารถติดต่อได้อย่างเพียงพอ	✓	✓	N/A
	(4.2) การกำหนดระยะเวลาของกระบวนการดูแลลูกค้า	✓	✓	✓	N/A
	(4.3) การดูแลลูกค้า	✓	✓	✓	N/A
	(4.4) การรายงานเหตุการณ์ภัยทุจริตดิจิทัล และการสื่อสารต่อสาธารณชน	✓	✓	✓	N/A
5.3.3 การแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับภัยทุจริตดิจิทัล		✓	✓	✓	✓

หลักเกณฑ์	บริษัทเงินทุน และบริษัท เครดิตฟองซิเอร์	ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ที่ไม่มีบริการโอนเงินไปยังบัญชีของบุคคลอื่นที่มีอยู่กับผู้ให้บริการทางการเงินอื่น	ผู้ประกอบธุรกิจบริการโอนเงินด้วยวิธีการทางอิเล็กทรอนิกส์	ผู้ประกอบธุรกิจระบบโอนเงินรายย่อยระหว่างผู้ใช้บริการของระบบ
5.3.4 การสร้างความตระหนักรู้ถึงภัยทุจริตดิจิทัล				
(1) การสร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัล	N/A	N/A	N/A	N/A
(2) การจัดให้มีการประเมินความตระหนักรู้ต่อภัยทุจริตดิจิทัล (awareness test)	N/A	N/A	N/A	N/A
5.3.5 การรายงานข้อมูลต่อธนาคารแห่งประเทศไทย	✓	✓	✓	✓
5.3.6 การเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษ	✓	✓	✓	✓

✓ ให้ปฏิบัติตามที่กำหนดไว้ในหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management)

N/A ไม่ต้องถือปฏิบัติตามหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management) สำหรับเรื่องดังกล่าว