ประกาศธนาคารแห่งประเทศไทย

ที่ ๕๐/๒๕๖๙

เรื่อง หลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management) ของสถาบันการเงินเฉพาะกิจ

---

๑. เหตุผลในการออกประกาศ

เนื่องจากภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงินมีหลากหลายรูปแบบ ไม่ว่าจะเป็นการสวมรอยทำธุรกรรมแทนลูกค้า (unauthorized payment fraud) หรือการหลอกลวงหรือข่มขู่ลูกค้าให้โอนเงินแก่มิจฉาชีพด้วยตนเอง (authorized payment fraud) ก่อให้เกิดความเสียหายต่อประชาชนในวงกว้างและกระทบต่อระบบเศรษฐกิจโดยรวม ซึ่งธนาคารแห่งประเทศไทยตระหนักถึงความสำคัญในการบริหารจัดการภัยทุจริตดิจิทัลดังกล่าว จึงได้ออกหลักเกณฑ์และมาตรการต่าง ๆ ให้สถาบันการเงินเฉพาะกิจถือปฏิบัติมาอย่างต่อเนื่อง ประกอบด้วยการออกหลักเกณฑ์ว่าด้วยมาตรฐานและมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีสำหรับสถาบันการเงิน ตามอำนาจหน้าที่ที่กำหนดในพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ และการออกหลักเกณฑ์เพื่อยกระดับการกำกับดูแลของธนาคารแห่งประเทศไทยในการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงินเฉพาะกิจ เพื่อเป็นการป้องกันประชาชนจากการตกเป็นเหยื่อของมิจฉาชีพในรูปแบบการสวมรอยทำธุรกรรมแทนลูกค้า อย่างไรก็ตาม ปัจจุบันมิจฉาชีพมีรูปแบบ วิธีการ และเทคนิคที่หลากหลายมากยิ่งขึ้น โดยเฉพาะรูปแบบการหลอกลวงหรือข่มขู่ลูกค้าให้โอนเงินแก่มิจฉาชีพด้วยตนเอง ที่ยังคงเป็นปัญหาสำคัญของประเทศไทย โดยมิจฉาชีพมีการใช้บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ของตนเองหรือผู้อื่นเป็นเครื่องมือในการรับเงินและถ่ายโอนเงินที่ได้จากการกระทำความผิด ส่งผลให้ประชาชนจำนวนมากได้รับความเดือดร้อนต้องสูญเสียเงินจำนวนมากให้กับมิจฉาชีพ

ในครั้งนี้ ธนาคารแห่งประเทศไทยได้ออกประกาศหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management) ของสถาบันการเงินเฉพาะกิจ เพื่อยกระดับการปฏิบัติตามแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน และหนังสือเวียน เรื่อง การเพิ่มความเข้มงวดในการจัดการบัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์ในกรณีลูกค้ามีความเสี่ยงสูงหรือใช้บัญชีที่มีลักษณะหรือพฤติกรรมผิดปกติ ให้มีความครอบคลุมและมีประสิทธิผลมากขึ้น โดยให้สถาบันการเงินเฉพาะกิจถือปฏิบัติในการบริหารจัดการภัยทุจริตดิจิทัลตั้งแต่ต้นจนจบกระบวนการ (end-to-end) เริ่มตั้งแต่การป้องกัน ติดตามและตรวจจับ จัดการและแก้ไขเมื่อเกิดเหตุภัยทุจริตดิจิทัล รวมทั้งดูแลลูกค้าที่ได้รับผลกระทบจากภัยทุจริตดิจิทัลดังกล่าว เพื่อให้การบริหารจัดการภัยทุจริตดิจิทัลเป็นไปอย่างมีประสิทธิผลสอดรับกับสภาพแวดล้อมทางการเงินที่เปลี่ยนแปลงไป ช่วยป้องกันและลดความเสียหายที่จะเกิดขึ้นกับประชาชนและรักษาความเชื่อมั่นในระบบสถาบันการเงินและระบบการชำระเงินของประเทศ

๒. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา ๑๒๐/๑ แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑ และที่แก้ไขเพิ่มเติม ธนาคารแห่งประเทศไทยโดยความเห็นชอบของรัฐมนตรีว่าการกระทรวงการคลัง ออกหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัลให้สถาบันการเงินเฉพาะกิจถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

๓. แนวนโยบายและหนังสือเวียนที่ยกเลิก

๓.๑ แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ลงวันที่ ๒๙ มีนาคม ๒๕๖๖ เฉพาะส่วนที่เกี่ยวข้องกับสถาบันการเงินเฉพาะกิจ

๓.๒ หนังสือเวียนที่ ธปท.ฝตท. (๐๑) ว. ๓๘๔/๒๕๖๗ เรื่อง การเพิ่มความเข้มงวดในการจัดการบัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์ในกรณีลูกค้ามีความเสี่ยงสูงหรือใช้บัญชีที่มีลักษณะหรือพฤติกรรมผิดปกติ ลงวันที่ ๓๑ พฤษภาคม ๒๕๖๗

๔. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับสถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ได้แก่ ธนาคารออมสิน ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ธนาคารอาคารสงเคราะห์ ธนาคารอิสลามแห่งประเทศไทย ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย และธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

๕. เนื้อหา

๕.๑ คำจำกัดความ

ในประกาศฉบับนี้

“ภัยทุจริตดิจิทัล (Digital Fraud)” หมายความว่า ภัยจากการทำธุรกรรมทางการเงินที่เกิดจากการกระทำความผิดหรือพยายามกระทำความผิดผ่านช่องทางดิจิทัลโดยทุจริต

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

“ลูกค้า” หมายความว่า บุคคลธรรมดา นิติบุคคล หรือบุคคลที่มีการตกลงกันทางกฎหมาย ซึ่งสร้างความสัมพันธ์ทางธุรกิจหรือทำธุรกรรมกับสถาบันการเงินเฉพาะกิจ

“บัญชี” หมายความว่า บัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์

“การทำธุรกรรมทางการเงิน” หมายความว่า การทำธุรกรรมทางการเงินที่สถาบันการเงินเฉพาะกิจให้บริการ 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 มาตรฐานอุตสาหกรรมที่สถาบันการเงินเฉพาะกิจได้ร่วมกันจัดทำเพื่อเป็นแนวปฏิบัติในการบริหารจัดการภัยทุจริตดิจิทัล

๕.๒ หลักการ

สถาบันการเงินเฉพาะกิจต้องมีการบริหารจัดการภัยทุจริตดิจิทัลอย่างเหมาะสมและทันกาลกับรูปแบบ วิธีการ และเทคนิคการทุจริตที่มีการเปลี่ยนแปลงไป โดยดำเนินการในแนวทางที่เป็นประโยชน์ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และเป็นการป้องกันและลดความเสียหายที่จะเกิดขึ้นกับประชาชนอย่างมีประสิทธิผล โดยต้องพิจารณาให้เกิดความสมดุลระหว่างความสะดวกและความปลอดภัยในการทำธุรกรรมทางการเงิน และคำนึงถึงการคุ้มครองลูกค้าอย่างเป็นธรรมด้วย

๕.๓ หลักเกณฑ์

๕.๓.๑ การกำหนดนโยบายและการกำกับดูแลการบริหารจัดการภัยทุจริตดิจิทัล

คณะกรรมการของสถาบันการเงินเฉพาะกิจและผู้บริหารในตำแหน่งสูงสุดของสถาบันการเงินเฉพาะกิจต้องกำกับดูแลให้สถาบันการเงินเฉพาะกิจมีการบริหารจัดการภัยทุจริตดิจิทัลที่เหมาะสมกับรูปแบบ วิธีการ เทคนิคการทุจริตและผลกระทบของภัยทุจริตดิจิทัลที่เกิดขึ้น และมีการแก้ไขสถานการณ์ที่ทันกาล เพื่อป้องกันและลดความเสียหายที่จะเกิดขึ้นกับลูกค้า ตั้งแต่ต้นจนจบกระบวนการ โดยเริ่มตั้งแต่การป้องกัน ติดตามและตรวจจับ จัดการและแก้ไขเมื่อเกิดเหตุภัยทุจริตดิจิทัล รวมทั้งดูแลลูกค้าที่ได้รับผลกระทบจากภัยทุจริตดังกล่าว โดยกำหนดให้เป็นความเสี่ยงสำคัญที่องค์กรต้องมีการบริหารจัดการร่วมกันแบบบูรณาการ โดยสถาบันการเงินเฉพาะกิจต้องดำเนินการ ดังนี้

(๑) กำหนดให้มีคณะทำงานหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทำหน้าที่กำหนดนโยบายและกำกับดูแลการบริหารจัดการภัยทุจริตดิจิทัล เพื่อให้องค์กรให้ความสำคัญและมีแนวทางบริหารจัดการภัยทุจริตดิจิทัลที่เหมาะสม ทันกาล และมีประสิทธิผลอย่างต่อเนื่องสอดรับกับบริบทของปัญหาภัยทุจริตในแต่ละช่วงเวลา และสามารถลดความเสียหายที่จะเกิดขึ้นกับลูกค้าได้ทันท่วงที

(๒) กำหนดนโยบายการบริหารจัดการภัยทุจริตดิจิทัลที่ชัดเจนเป็นลายลักษณ์อักษรโดยได้รับความเห็นชอบจากคณะกรรมการของสถาบันการเงินเฉพาะกิจ และนโยบายดังกล่าวต้องสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง บริบทของปัญหาภัยทุจริตดิจิทัลในแต่ละช่วงเวลาและครอบคลุมอย่างน้อย ดังนี้

(๒.๑) บทบาทหน้าที่ของคณะทำงาน หรือผู้บริหารระดับสูงที่ได้รับมอบหมายและหน่วยงานที่รับผิดชอบ เพื่อผลักดันให้มีการบริหารจัดการภัยทุจริตดิจิทัลที่มีประสิทธิผล

โดยครอบคลุมตั้งแต่ต้นจนจบกระบวนการ รวมทั้งประเมินความพร้อมขององค์กรทั้งในด้านบุคลากร กระบวนการ เทคโนโลยีและเครื่องมือที่ใช้ในการจัดการภัยทุจริตดิจิทัลอย่างสม่ำเสมอ

(๒.๒) แนวทางและกระบวนการบริหารจัดการภัยทุจริตดิจิทัลตั้งแต่ต้นจนจบกระบวนการ เพื่อให้การบริหารจัดการภัยทุจริตดิจิทัลเป็นไปอย่างมีประสิทธิผล

(๒.๓) การติดตามและวัดประสิทธิผลของการจัดการภัยทุจริตดิจิทัลอย่างต่อเนื่อง เพื่อทบทวนและปรับปรุงแนวทางและกระบวนการบริหารจัดการภัยทุจริตดิจิทัลให้เหมาะสมกับสถานการณ์อยู่เสมอ

ทั้งนี้ สถาบันการเงินเฉพาะกิจต้องจัดให้มีการทบทวนและปรับปรุงนโยบายการบริหารจัดการภัยทุจริตดิจิทัลอย่างสม่ำเสมอ โดยเฉพาะเมื่อมีเหตุการณ์หรือการเปลี่ยนแปลงที่ส่งผลกระทบต่อประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัลอย่างมีนัยสำคัญหรือตามความถี่ที่เหมาะสม ทั้งนี้ หากเป็นการปรับปรุงที่มีนัยสำคัญ ต้องได้รับความเห็นชอบจากคณะกรรมการของสถาบันการเงินเฉพาะกิจ และหากเป็นการปรับปรุงที่ไม่มีนัยสำคัญ คณะทำงานหรือผู้บริหารระดับสูงที่ได้รับมอบหมายสามารถดำเนินการได้โดยต้องรายงานคณะกรรมการของสถาบันการเงินเฉพาะกิจเพื่อทราบในภายหลังด้วย

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

(๔) จัดให้มีการสื่อสารเผยแพร่นโยบายและแนวทางการบริหารจัดการภัยทุจริตดิจิทัลให้ทุกฝ่ายงานที่เกี่ยวข้องในองค์กรนำไปปฏิบัติได้อย่างเหมาะสม รวมทั้งพัฒนาองค์ความรู้ของบุคลากรในองค์กรเกี่ยวกับการบริหารจัดการภัยทุจริตดิจิทัลอย่างต่อเนื่อง เพื่อให้พนักงานที่เกี่ยวข้องทุกระดับมีความรู้ความเข้าใจที่เพียงพอในการกำกับดูแลและการบริหารจัดการภัยทุจริตดิจิทัลรูปแบบใหม่ ๆ ที่อาจเกิดขึ้น

(๕) จัดให้หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง หน่วยงานที่ทำหน้าที่กำกับการปฏิบัติตามกฎเกณฑ์ และหน่วยงานที่ทำหน้าที่ตรวจสอบภายใน ต้องมีส่วนร่วมในการผลักดันให้องค์กรมีกระบวนการควบคุมดูแลความเสี่ยงที่ดี เพื่อให้การบริหารจัดการภัยทุจริตดิจิทัลขององค์กรดำเนินการได้อย่างเหมาะสมและทันกาล

(๖) กำหนดเป้าหมายและตัวชี้วัดในการประเมินประสิทธิผลของการจัดการภัยทุจริตดิจิทัลที่ชัดเจนและวัดผลได้จริง ครอบคลุมตั้งแต่ต้นจนจบกระบวนการ และต้องปรับปรุงเป้าหมาย

และตัวชี้วัดดังกล่าวอย่างสม่ำเสมอเพื่อให้สอดคล้องกับรูปแบบ วิธีการ และเทคนิคการทุจริตของภัยทุจริตดิจิทัลที่เปลี่ยนแปลงไป

(๗) ติดตามและประเมินประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัล รวมทั้งปรับปรุงระบบงาน กระบวนการ และผลิตภัณฑ์หรือบริการทางการเงิน ให้ครอบคลุมรูปแบบ วิธีการ และเทคนิคการทุจริตของภัยทุจริตดิจิทัลที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง เพื่อให้สามารถตรวจจับและจัดการธุรกรรมที่มีความผิดปกติได้ทันท่วงที โดยผู้บริหารในตำแหน่งสูงสุด คณะทำงาน หรือผู้บริหารระดับสูงที่ได้รับมอบหมายต้องจัดให้มีการรายงานประเด็นที่มีนัยสำคัญต่อคณะกรรมการของสถาบันการเงินเฉพาะกิจอย่างสม่ำเสมอ

(๘) สนับสนุนการจัดทำมาตรฐานอุตสาหกรรม โดยให้ครอบคลุมกระบวนการบริหารจัดการภัยทุจริตดิจิทัลที่จำเป็นและสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง เพื่อให้มั่นใจว่ากระบวนการบริหารจัดการภัยทุจริตดิจิทัลมีมาตรฐานเดียวกัน

๕.๓.๒ กระบวนการจัดการภัยทุจริตดิจิทัล

สถาบันการเงินเฉพาะกิจต้องจัดให้มีกรอบการดำเนินการบริหารจัดการภัยทุจริตดิจิทัลที่ชัดเจนตลอดวงจรการใช้บริการของลูกค้า เริ่มตั้งแต่ลูกค้าสมัครใช้บริการหรือเปิดบัญชีทำธุรกรรมทางการเงิน จนถึงปิดบัญชี ยกเลิกการใช้บริการ หรือยุติความสัมพันธ์ โดยต้องครอบคลุมกระบวนการอย่างน้อย ดังนี้

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

สถาบันการเงินเฉพาะกิจต้องดำเนินการตามกระบวนการรู้จักลูกค้า (Know Your Customer: KYC) โดยระบุและพิสูจน์ทราบตัวตนของลูกค้าจากแหล่งข้อมูลที่น่าเชื่อถือ เพื่อให้มั่นใจว่าข้อมูลที่ได้รับจากลูกค้าเป็นข้อมูลที่แท้จริง มีความถูกต้อง และเป็นปัจจุบัน รวมถึงต้องสอบถามวัตถุประสงค์ในการเปิดบัญชีของลูกค้า และวิเคราะห์ลักษณะหรือพฤติการณ์ของลูกค้าร่วมด้วย และต้องดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าเมื่อเริ่มทำธุรกรรมครั้งแรก และตรวจสอบเป็นระยะจนสิ้นสุดเมื่อมีการปิดบัญชีหรือยุติความสัมพันธ์กับลูกค้าตามหลักเกณฑ์ของกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินและประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การบริหารจัดการความเสี่ยงจากการใช้บริการทางการเงินของลูกค้าสำหรับสถาบันการเงินเฉพาะกิจ โดยหากสถาบันการเงินเฉพาะกิจพบว่าลูกค้ามีความเสี่ยงต่อการนำบัญชีไปใช้เป็นบัญชีม้า เช่น มีพฤติกรรมการใช้บัญชีที่ไม่สอดคล้องกับข้อมูลของลูกค้า หรืออยู่ในรายชื่อบุคคลที่มีความเสี่ยงที่ได้รับจากฐานข้อมูลที่น่าเชื่อถือ สถาบันการเงินเฉพาะกิจต้องยกระดับการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าให้อยู่ในระดับที่เข้มข้น (Enhanced Customer Due Diligence: EDD) โดยตรวจสอบข้อมูลอื่นเพิ่มเติม เช่น แหล่งที่มาของเงินหรือทรัพย์สิน แหล่งที่มาของฐานะความมั่งคั่ง รวมถึงข้อมูลเกี่ยวกับการประกอบกิจการของลูกค้า อาชีพ ชื่อและสถานที่ตั้งของที่ทำงาน

ทั้งนี้ สถาบันการเงินเฉพาะกิจต้องนำข้อมูลที่ได้จากการรู้จักลูกค้า การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า และจากฐานข้อมูลที่น่าเชื่อถือ มาประเมินและจัดกลุ่มลูกค้าตามระดับความเสี่ยงที่ลูกค้าอาจนำบัญชีไปใช้เป็นบัญชีม้าหรืออาจถูกหลอกลวงจนเกิดความเสียหาย รวมทั้งทบทวนระดับความเสี่ยงของลูกค้าให้เป็นปัจจุบันและเหมาะสมกับบริบทที่เปลี่ยนแปลงไปอยู่เสมอ

(๒) การติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงิน (monitoring and detection)

สถาบันการเงินเฉพาะกิจต้องมีกระบวนการติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงินในเชิงรุกอย่างมีประสิทธิผล ครอบคลุมรูปแบบของภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงินที่เปลี่ยนแปลงไปอย่างต่อเนื่อง โดยต้องสามารถประเมินระดับความเสี่ยงของบัญชี ทั้งบัญชีของบุคคลที่คาดว่าจะได้รับความเสียหายจากภัยทุจริตดิจิทัลและบุคคลที่มีความเสี่ยงในการนำบัญชีไปใช้เป็นบัญชีม้า รวมถึงตรวจจับการทำธุรกรรมและการใช้บัญชีที่มีความผิดปกติได้อย่างทันท่วงที เพื่อให้มีการจัดการภัยทุจริตดิจิทัลที่เหมาะสมและทันกาล ซึ่งจะมีส่วนทำให้สามารถป้องกันและจำกัดความเสียหายที่เกิดจากภัยทุจริตดิจิทัลไม่ให้ขยายตัวหรือลุกลามเป็นวงกว้าง ดังนี้

(๒.๑) จัดให้มีระบบการติดตามและตรวจจับธุรกรรมที่ผิดปกติได้ทันท่วงที โดยต้องกำหนดเงื่อนไขในการติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงินทั้งธุรกรรมของบุคคลที่คาดว่าจะได้รับความเสียหายจากภัยทุจริตดิจิทัลและบุคคลที่มีความเสี่ยงในการนำบัญชีไปใช้เป็นบัญชีม้า โดยต้องพิจารณาถึงรูปแบบของภัยทุจริตดิจิทัลที่มีการเปลี่ยนแปลงอย่างต่อเนื่องทั้งที่เกิดขึ้นภายในประเทศไทยและในต่างประเทศ ช่องทางการให้บริการ พฤติกรรมการใช้บัญชี ข้อมูลพฤติกรรมต้องสงสัยที่สถาบันการเงินเฉพาะกิจตรวจพบเอง ข้อมูลที่ได้รับจากผู้ให้บริการทางการเงินแห่งอื่น ข้อมูลจากระบบ Central Fraud Registry (CFR) และข้อมูลจากหน่วยงานอื่น ๆ

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

(๓) การจัดการภัยทุจริตดิจิทัล (actions)

สถาบันการเงินเฉพาะกิจต้องมีการป้องกัน จำกัด และระงับความเสียหายจากภัยทุจริตดิจิทัลอย่างรวดเร็ว เพียงพอและเหมาะสม สอดคล้องตามระดับความเสี่ยงของธุรกรรมทางการเงิน ซึ่งประกอบด้วยการป้องกันและจำกัดความเสียหายให้แก่ลูกค้า และการจัดการบัญชีที่อาจเข้าข่ายเป็นบัญชีม้าเพื่อจำกัดและระงับความเสียหาย โดยต้องจัดให้มีการจัดการอย่างน้อย ดังนี้

(๓.๑) การป้องกันและจำกัดความเสียหายให้แก่ลูกค้า

สถาบันการเงินเฉพาะกิจต้องจัดให้มีการป้องกันและจำกัดความเสียหายแก่ลูกค้าอย่างเพียงพอและเหมาะสมตามระดับความเสี่ยงของการทำธุรกรรมทางการเงิน เช่น มีกระบวนการยืนยันตัวตนลูกค้า (authentication) ที่รัดกุมและเหมาะสมกับความเสี่ยงของลูกค้า ธุรกรรม ผลิตภัณฑ์และบริการ และช่องทางการให้บริการ การแจ้งเตือน หน่วง หรือระงับการทำธุรกรรมที่มีความผิดปกติตามระดับความเสี่ยงของธุรกรรม รวมถึงการกำหนดวงเงินการทำธุรกรรมของลูกค้าให้เหมาะสมกับระดับความเสี่ยงและสอดคล้องกับการใช้งานตามปกติของลูกค้า เพื่อลดความเสียหายจากภัยทุจริตดิจิทัล

(๓.๒) การจัดการบัญชีที่อาจเข้าข่ายเป็นบัญชีม้าเพื่อจำกัดและระงับความเสียหาย

สถาบันการเงินเฉพาะกิจต้องจัดให้มีการจำกัดและระงับความเสียหายและผลกระทบของความเสียหายให้สอดคล้องกับระดับความเสี่ยงของบุคคลที่นำบัญชีไปใช้เป็นบัญชีม้าหรืออาจนำบัญชีไปใช้เป็นบัญชีม้าได้อย่างเหมาะสมและทันกาล เช่น การระงับเงินเข้า การระงับเงินออก การระงับการให้บริการผ่านช่องทางอิเล็กทรอนิกส์ การปฏิเสธการเปิดบัญชีใหม่ และการควบคุมการถอนเงินสด

(๔) การแก้ไขสถานการณ์และการดูแลลูกค้า (response)

สถาบันการเงินเฉพาะกิจต้องแก้ไขสถานการณ์และดูแลลูกค้าเมื่อเกิดเหตุการณ์ภัยทุจริตดิจิทัลอย่างชัดเจน รวดเร็ว และเป็นธรรม โดยขั้นต่ำต้องดำเนินการ ดังนี้

(๔.๑) การจัดให้มีช่องทางรับแจ้งเหตุการณ์ต้องสงสัยหรือเหตุการณ์ภัยทุจริตดิจิทัล

สถาบันการเงินเฉพาะกิจต้องจัดให้มีช่องทางติดต่อเร่งด่วน (hotline) ทางโทรศัพท์ หรือทางอิเล็กทรอนิกส์เพื่อให้ลูกค้าสามารถติดต่อสถาบันการเงินเฉพาะกิจได้โดยช่องทางดังกล่าวจะต้องเพียงพอและให้บริการอย่างต่อเนื่องทั้งในและนอกเวลาทำการ (๒๔ x ๗) เพื่อให้ลูกค้าสามารถแจ้งเหตุการณ์ต้องสงสัยหรือเหตุการณ์ที่เป็นภัยทุจริตดิจิทัลได้โดยสะดวกและรวดเร็ว ทั้งนี้ หลังได้รับแจ้งเหตุดังกล่าว สถาบันการเงินเฉพาะกิจต้องเร่งดำเนินการตามกฎหมายและหลักเกณฑ์อื่นที่เกี่ยวข้องอย่างเคร่งครัด เพื่อให้การติดตามตรวจสอบเหตุการณ์เป็นไปอย่างทันกาลและจำกัดความเสียหายที่อาจเกิดขึ้น

(๔.๒) การกำหนดระยะเวลาของกระบวนการดูแลลูกค้า

สถาบันการเงินเฉพาะกิจต้องกำหนดระยะเวลาของกระบวนการดูแลลูกค้าที่ได้รับความเสียหายที่เกิดขึ้นจากภัยทุจริตดิจิทัลให้ชัดเจน เช่น การแจ้งให้ลูกค้าที่เกี่ยวข้องทราบเมื่อเกิดเหตุการณ์ การติดต่อกลับไปยังลูกค้าดังกล่าวอย่างรวดเร็วภายในเวลาที่เหมาะสมภายหลังลูกค้าแจ้งสถาบันการเงินเฉพาะกิจเกี่ยวกับเหตุการณ์ที่อาจเข้าข่ายเป็นภัยทุจริตดิจิทัล ทั้งนี้

กระบวนการดูแลลูกค้ารวมถึงกระบวนการสื่อสารและการทำความเข้าใจกับลูกค้าเกี่ยวกับปัญหาและผลกระทบที่เกิดขึ้นอย่างทันกาล

(๔.๓) การดูแลลูกค้า

สถาบันการเงินเฉพาะกิจต้องดูแลลูกค้าที่ได้รับความเสียหายจากภัยทุจริตดิจิทัลอย่างเหมาะสม รวดเร็ว และเป็นธรรม โดยสถาบันการเงินเฉพาะกิจต้องจัดให้มีผู้รับผิดชอบดูแลและประสานงานอย่างชัดเจน นอกจากนี้ หากการจัดการภัยทุจริตดิจิทัลของสถาบันการเงินเฉพาะกิจก่อให้เกิดผลกระทบต่อลูกค้าที่ไม่มีส่วนเกี่ยวข้องกับการกระทำทุจริต สถาบันการเงินเฉพาะกิจต้องแก้ไขปัญหาที่เกิดจากผลกระทบดังกล่าวที่รวดเร็ว เช่น การปลดการระงับบัญชีโดยเร็วภายหลังจากที่ได้รับคำสั่งจากหน่วยงานทางการหรือเมื่อได้ดำเนินการพิจารณาตามกระบวนการหรือหลักเกณฑ์ของสถาบันการเงินเฉพาะกิจแล้ว การเยียวยาความเสียหายให้แก่ลูกค้าอย่างรวดเร็วเมื่อพิสูจน์ได้ว่าลูกค้าได้รับความเสียหายจากความบกพร่องของสถาบันการเงินเฉพาะกิจ หรือเมื่อได้รับคำสั่งจากหน่วยงานที่เกี่ยวข้อง

(๔.๔) การรายงานเหตุการณ์ภัยทุจริตดิจิทัล และการสื่อสารต่อสาธารณชน

สถาบันการเงินเฉพาะกิจต้องรายงานเหตุการณ์ภัยทุจริตดิจิทัลแก่คณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย ให้เหมาะสมตามระดับความรุนแรงของเหตุการณ์ ทั้งนี้ กรณีที่เกิดความเสียหายกับลูกค้าในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของสถาบันการเงินเฉพาะกิจ สถาบันการเงินเฉพาะกิจต้องรายงานเหตุการณ์ภัยทุจริตดิจิทัลให้ธนาคารแห่งประเทศไทยทราบโดยเร็วตามช่องทางที่กำหนด

นอกจากนี้ ในกรณีที่เกิดเหตุการณ์ภัยทุจริตดิจิทัลกับลูกค้าของสถาบันการเงินเฉพาะกิจหรือผู้ประกอบธุรกิจอื่นหลายแห่งพร้อมกันและส่งผลกระทบในวงกว้างต่อความเชื่อมั่นของระบบการเงินหรือระบบการชำระเงิน สถาบันการเงินเฉพาะกิจที่ลูกค้าของตนได้รับผลกระทบจากภัยทุจริตดิจิทัลดังกล่าวควรร่วมกับสถาบันการเงินเฉพาะกิจอื่น ผู้ประกอบธุรกิจอื่น สมาคมของสถาบันการเงินเฉพาะกิจ สมาคมของผู้ประกอบธุรกิจ และหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับเหตุการณ์ดังกล่าว จัดให้มีการสื่อสารเพื่อชี้แจงและทำความเข้าใจกับลูกค้าโดยเร็ว และกำหนดแนวทางช่วยเหลือและดูแลลูกค้าให้เป็นมาตรฐานเดียวกัน

๕.๓.๓ การแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับภัยทุจริตดิจิทัล

สถาบันการเงินเฉพาะกิจต้องจัดให้มีกลไกการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับภัยทุจริตดิจิทัลระหว่างสถาบันการเงินเฉพาะกิจ ผู้ให้บริการทางการเงิน และหน่วยงานอื่นที่เกี่ยวข้อง เพื่อให้สามารถร่วมกันบริหารการจัดการภัยทุจริตดิจิทัลได้อย่างทันกาล อันจะช่วยลดโอกาสในการเกิดความเสียหายต่อลูกค้าอย่างมีประสิทธิผล โดยต้องดำเนินการอย่างน้อย ดังนี้

(๑) จัดให้มีกลไกการแลกเปลี่ยนข้อมูลที่สามารถส่งผ่านข้อมูลได้อย่างถูกต้องและรวดเร็ว เพื่อป้องกัน ติดตามและตรวจจับ จัดการและแก้ไขเหตุภัยทุจริตดิจิทัล โดยต้องเป็นไป

ตามแนวทางที่กำหนดในกฎหมายว่าด้วยมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี รวมถึงกฎหมายหรือหลักเกณฑ์อื่นที่เกี่ยวข้องด้วย

(๒) สนับสนุนข้อมูลที่ต้องใช้ในการสืบสวนสอบสวนและติดตามหาผู้กระทำความผิดให้แก่พนักงานสอบสวนที่ได้รับมอบหมายอย่างทันกาลตามที่พนักงานสอบสวนร้องขอ โดยสถาบันการเงินเฉพาะกิจต้องจัดให้มีผู้รับผิดชอบดูแลและประสานงานอย่างชัดเจน

๕.๓.๔ การสร้างความตระหนักรู้ถึงภัยทุจริตดิจิทัล

สถาบันการเงินเฉพาะกิจมีหน้าที่ในการสร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัลให้แก่ลูกค้า เพื่อป้องกันและลดโอกาสเกิดความเสียหาย ดังนี้

(๑) สร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัลในเชิงรุกให้แก่ลูกค้าในวงกว้างและสม่ำเสมอ ด้วยวิธีที่เกิดผลอย่างเป็นรูปธรรมผ่านช่องทางที่ลูกค้าสามารถเข้าถึงได้ง่าย เช่น การแจ้งเตือนผ่านแอปพลิเคชันที่ติดตั้งบนอุปกรณ์เคลื่อนที่ การจัดทำสื่อ infographic บนสื่อสังคมออนไลน์ โดยมีเนื้อหาครอบคลุมรูปแบบต่าง ๆ ของภัยทุจริตดิจิทัลที่เกิดขึ้นในปัจจุบัน วิธีการป้องกัน และแนวทางการแจ้งปัญหาเมื่อเกิดเหตุภัยทุจริตดิจิทัล เพื่อให้ลูกค้าโดยเฉพาะกลุ่มเปราะบางเกิดความเข้าใจและเพิ่มความระมัดระวังในการทำธุรกรรมทางการเงิน รวมทั้งให้การสนับสนุนหน่วยงานอื่นที่เกี่ยวข้องในการสร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัลให้แก่ลูกค้าและประชาชน

(๒) ธนาคารแห่งประเทศไทยสนับสนุนให้สถาบันการเงินเฉพาะกิจจัดให้มีการประเมินความตระหนักรู้ต่อภัยทุจริตดิจิทัล (awareness test) ของลูกค้า โดยรูปแบบของการประเมินต้องคำนึงถึงประสิทธิผลของการสร้างความตระหนักรู้ให้กับลูกค้า และมีการพัฒนารูปแบบของการประเมินอย่างต่อเนื่องให้สอดคล้องกับพฤติกรรมการหลอกลวงของมิจฉาชีพที่เปลี่ยนแปลงไป เพื่อเพิ่มภูมิคุ้มกันของลูกค้าสำหรับรูปแบบภัยทุจริตดิจิทัลต่าง ๆ โดยอาจพิจารณานำผลการประเมินไปใช้ประกอบการจัดทำกระบวนการป้องกันภัยทุจริตดิจิทัลให้มีประสิทธิผลยิ่งขึ้น เช่น ใช้เป็นปัจจัยเพิ่มเติมในการกำหนดระดับความเสี่ยงของลูกค้า การกำหนดความเข้มข้นในการสร้างความตระหนักรู้ หรือกำหนดค่าเริ่มต้นของวงเงินการทำธุรกรรมต่อวัน

๕.๓.๕ การรายงานข้อมูลต่อธนาคารแห่งประเทศไทย

สถาบันการเงินเฉพาะกิจต้องจัดทำและจัดส่งแบบรายงาน เพื่อประโยชน์ในการติดตามประเมินประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัลในภาพรวมและของสถาบันการเงินเฉพาะกิจ รวมทั้งความเหมาะสมของนโยบายทางการ ตามรูปแบบและระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนด รวมถึงจัดทำและจัดส่งรายงานและข้อมูลอื่นเพิ่มเติมเป็นรายกรณีตามที่ธนาคารแห่งประเทศไทยร้องขอ

๕.๓.๖ การเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษ

กรณีที่กรรมการ ผู้จัดการ หรือผู้มีอำนาจในการจัดการของสถาบันการเงินเฉพาะกิจถูกเปรียบเทียบปรับหรือถูกกล่าวโทษอันเนื่องมาจากการไม่ควบคุมดูแลให้สถาบันการเงินเฉพาะกิจปฏิบัติตามประกาศฉบับนี้ ให้สถาบันการเงินเฉพาะกิจเปิดเผยข้อมูลการถูกเปรียบเทียบปรับ

หรือถูกกล่าวโทษดังกล่าวตามหลักเกณฑ์การเปิดเผยข้อมูลที่กำหนดในประกาศธนาคารแห่งประเทศไทย ว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct) โดยอนุโลม

อย่างไรก็ดี ในกรณีที่ธนาคารแห่งประเทศไทยเห็นว่าการเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษดังกล่าวอาจกระทบกับความปลอดภัยหรือความผาสุกของประชาชน หรือประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัล ธนาคารแห่งประเทศไทยอาจแจ้งสถาบันการเงินเฉพาะกิจไม่ให้เปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษดังกล่าวก็ได้

ทั้งนี้ ธนาคารแห่งประเทศไทยจะกำหนดแนวปฏิบัติขั้นต่ำสำหรับการบริหารจัดการภัยทุจริตดิจิทัลเพื่อให้สถาบันการเงินเฉพาะกิจใช้อ้างอิงในการดำเนินการหรือเป็นมาตรฐานขั้นต่ำในการปฏิบัติที่ถือเป็นการปฏิบัติตามหลักเกณฑ์เรื่องใดเรื่องหนึ่งของประกาศฉบับนี้ โดยเมื่อสถาบันการเงินเฉพาะกิจดำเนินการตามแนวปฏิบัติขั้นต่ำดังกล่าวแล้วให้ถือว่าเป็นการปฏิบัติตามหลักเกณฑ์เรื่องนั้น

๕.๔ การถือปฏิบัติตามหลักเกณฑ์ของสถาบันการเงินเฉพาะกิจ

ให้สถาบันการเงินเฉพาะกิจปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ เว้นแต่กรณีสถาบันการเงินเฉพาะกิจมีการให้บริการทางการเงินแก่ลูกค้าที่มีความเสี่ยงต่ำ หรือมีการทำธุรกรรมที่มีความเสี่ยงต่ำ ให้สถาบันการเงินเฉพาะกิจนำหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ไปปรับใช้ตามระดับความเสี่ยง (risk proportionality) ทั้งในกรณีที่บัญชีของลูกค้าอาจถูกนำไปใช้เป็นบัญชีม้าหรือลูกค้าอาจถูกหลอกลวงจนเกิดความเสียหาย โดยต้องคำนึงถึงขอบเขตการประกอบธุรกิจ กลุ่มลูกค้าที่ให้บริการ ประเภทของผลิตภัณฑ์ และช่องทางการให้บริการ

๖. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑ พฤศจิกายน ๒๕๖๙ เป็นต้นไป

ประกาศ ณ วันที่ ๗ ตุลาคม พ.ศ. ๒๕๖๙
วิทัย รัตนากร
ผู้ว่าการ
ธนาคารแห่งประเทศไทย