(ร่าง) ประกาศธนาคารแห่งประเทศไทย

ที่ xx /2568

เรื่อง การบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตร (Card Fraud Management)

---

1. เหตุผลในการออกประกาศ

ภัยทุจริตจากการทำธุรกรรมทางการเงินมีหลากหลายรูปแบบมากขึ้นทั้งในลักษณะที่ผู้ใช้บริการไม่ได้ทำธุรกรรมด้วยตนเองหรือถูกสวมรอยทำธุรกรรมแทนตนเอง (unauthorized payment fraud) และลักษณะที่ผู้ใช้บริการถูกหลอกลวงให้หลงเชื่อและทำธุรกรรมให้มิจฉาชีพ (authorized payment fraud) อันก่อให้เกิดความเสียหายต่อประชาชนในวงกว้างและส่งผลกระทบต่อระบบเศรษฐกิจการเงินและระบบการชำระเงินโดยรวม ซึ่งปัจจุบัน ภัยทุจริตได้ขยายจากการใช้บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์มายังบริการชำระเงินอื่นมากขึ้น ซึ่งบัตรเครดิต บัตรเดบิต บัตรเอทีเอ็มและบัตรเงินอิเล็กทรอนิกส์ เป็นเครื่องมือการชำระเงินอย่างหนึ่งที่อาจถูกนำมาใช้ในการกระทำความผิด อันเนื่องจากมีผู้ใช้บริการเป็นจำนวนมากและมีการใช้งานกันอย่างแพร่หลายเพื่อใช้ชำระค่าสินค้าและบริการ หรือใช้ในการเบิก ถอน โอน หรือทำธุรกรรมอื่นใดแทนการใช้เงินสด

ธนาคารแห่งประเทศไทยจึงกำหนดหลักเกณฑ์การบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตร เพื่อให้ผู้ให้บริการที่เกี่ยวข้องกับการทำธุรกรรมด้วยบัตรยกระดับความปลอดภัยในการใช้งานบัตร การบริหารจัดการภัยทุจริต และการดูแลประชาชนผู้ใช้บริการที่ได้รับความเสียหายจากภัยทุจริต โดยมีการป้องกัน การติดตามและตรวจจับธุรกรรม การจัดการและการดูแลผู้ใช้บริการ การสร้างความตระหนักรู้ และความร่วมมือระหว่างกันของผู้ที่เกี่ยวข้อง อย่างเพียงพอเหมาะสม มีมาตรฐาน และเกิดประสิทธิผลมากขึ้น ซึ่งจะช่วยให้ประชาชนได้รับความปลอดภัยในการทำธุรกรรมยิ่งขึ้นและได้รับการช่วยเหลือดูแลอย่างรวดเร็วเมื่อเกิดปัญหา ตลอดจนรักษาความเชื่อมั่นต่อระบบการชำระเงิน และระบบเศรษฐกิจการเงินโดยรวมของประเทศ

2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 24 และมาตรา 26 แห่งพระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560 ธนาคารแห่งประเทศไทยกำหนดหลักเกณฑ์การบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตร ตามความในประกาศฉบับนี้

3. แนวนโยบายที่ยกเลิก

แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ฉบับลงวันที่ 29 มีนาคม 2566 เฉพาะในส่วนที่เกี่ยวข้องกับบริการบัตร และเอกสารแนบ 1 การบริหารจัดการภัยทุจริตจากการทำธุรกรรมการชำระเงินผ่านบัตร

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงินที่ได้รับอนุญาตประเภทการให้บริการบัตรเครดิต บัตรเดบิต หรือบัตรเอทีเอ็ม การให้บริการเงินอิเล็กทรอนิกส์ การให้บริการแก่ผู้รับบัตร และการให้บริการสนับสนุนบริการแก่ผู้รับบัตร รวมทั้งผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงินที่ได้รับอนุญาตประเภทการให้บริการระบบเครือข่ายบัตร

5. เนื้อหา

5.1 นิยาม

ในประกาศฉบับนี้

“ภัยทุจริต” หมายความว่า ภัยทุจริตจากการทำธุรกรรมด้วยบัตรที่เกิดจากการกระทำหรือพยายามกระทำความผิด โดยมีบัตรเป็นเครื่องมือในการใช้กระทำความผิด ซึ่งครอบคลุมทั้งกรณีที่ผู้ใช้บริการไม่ได้ทำธุรกรรมด้วยตนเองหรือถูกสวมรอยทำธุรกรรมแทนตนเอง (unauthorized payment fraud) และกรณีที่ผู้ใช้บริการถูกหลอกลวงให้หลงเชื่อและทำธุรกรรมให้มิจฉาชีพ (authorized payment fraud)

“ผู้ให้บริการออกบัตร” หมายความว่า ผู้ประกอบธุรกิจที่ได้รับอนุญาตให้ประกอบธุรกิจการให้บริการบัตรเครดิต บัตรเดบิต หรือบัตรเอทีเอ็ม และการให้บริการเงินอิเล็กทรอนิกส์ในรูปแบบบัตรที่ใช้บริการระบบเครือข่ายบัตร ตามกฎหมายว่าด้วยระบบการชำระเงิน

“ผู้ให้บริการรับบัตร” หมายความว่า ผู้ประกอบธุรกิจที่ได้รับอนุญาตให้ประกอบธุรกิจการให้บริการแก่ผู้รับบัตร และการให้บริการสนับสนุนบริการแก่ผู้รับบัตร ตามกฎหมายว่าด้วยระบบการชำระเงิน

“ผู้ให้บริการระบบเครือข่ายบัตร” หมายความว่า ผู้ประกอบธุรกิจที่ได้รับอนุญาตให้ประกอบธุรกิจการให้บริการระบบเครือข่ายบัตรตามกฎหมายว่าด้วยระบบการชำระเงิน

“บัตร” หมายความว่า บัตรเครดิต บัตรเดบิต บัตรเอทีเอ็ม หรือบัตรเงินอิเล็กทรอนิกส์ที่ใช้บริการผ่านระบบเครือข่ายบัตร ทั้งที่ให้บริการกับบุคคลธรรมดาและนิติบุคคล

“บัตรเครดิต” หมายความว่า บัตรอิเล็กทรอนิกส์ที่ผู้ให้บริการออกบัตรออกให้แก่ผู้ใช้บริการเพื่อใช้ชำระค่าสินค้า ค่าบริการ หรือค่าอื่นใด แทนการชำระด้วยเงินสด หรือเพื่อใช้เบิกถอน โอน หรือทำธุรกรรมอื่นใดที่เกี่ยวกับเงิน และผู้ให้บริการออกบัตรจะเรียกให้ผู้ใช้บริการชำระเงินในภายหลัง

“บัตรเดบิต” หมายความว่า บัตรอิเล็กทรอนิกส์ที่ผู้ให้บริการออกบัตรออกให้แก่ผู้ใช้บริการเพื่อใช้ชำระค่าสินค้า ค่าบริการ หรือค่าอื่นใด แทนการชำระด้วยเงินสด หรือเพื่อใช้เบิกถอน โอน หรือทำธุรกรรมอื่นใดที่เกี่ยวกับเงิน ตามมูลค่าของเงินที่ผู้ใช้บริการได้ฝากไว้กับผู้ให้บริการออกบัตร

“บัตรเอทีเอ็ม” หมายความว่า บัตรอิเล็กทรอนิกส์ที่ผู้ให้บริการออกบัตรออกให้แก่ผู้ใช้บริการเพื่อใช้เบิก ถอน โอน หรือทำธุรกรรมอื่นใดที่เกี่ยวกับเงิน ตามมูลค่าของเงินที่ผู้ใช้บริการได้ฝากไว้กับผู้ให้บริการออกบัตร

“บัตรเงินอิเล็กทรอนิกส์” หมายความว่า บัตรอิเล็กทรอนิกส์ที่ผู้ให้บริการออกบัตรออกให้แก่ผู้ใช้บริการ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยมีการชำระเงินให้แก่ผู้ให้บริการออกบัตรไว้ล่วงหน้าเพื่อนำไปใช้ชำระค่าสินค้า ค่าบริการ หรือค่าอื่นใด แทนการชำระด้วยเงินสด และได้มีการบันทึกมูลค่าหรือจำนวนเงินที่ชำระไว้ล่วงหน้า

“บัญชีม้า” หมายความว่า บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ ซึ่งถูกนำมาใช้หรืออาจถูกนำมาใช้เป็นเครื่องมือในการรับเงินและถ่ายโอนเงินที่ได้มาจากอาชญากรรมทางเทคโนโลยี

“ผู้บริหารระดับสูงสุด” หมายความว่า บุคคลซึ่งมีอำนาจสูงสุดที่มีหน้าที่และความรับผิดชอบในการวางแผน การกำกับ หรือการควบคุมกิจกรรม รวมถึงการจัดการและการบริหารงานขององค์กร

“ผู้บริหารระดับสูง” หมายความว่า บุคคลซึ่งมีอำนาจหน้าที่และความรับผิดชอบในการวางแผน การกำกับ หรือการควบคุมกิจกรรม รวมถึงการจัดการและการบริหารงานขององค์กร

“มาตรฐานอุตสาหกรรม” หมายความว่า มาตรฐานอุตสาหกรรมที่ผู้ให้บริการที่เกี่ยวข้องทั้งผู้ให้บริการออกบัตร ผู้ให้บริการรับบัตร และผู้ให้บริการระบบเครือข่ายบัตร ได้ร่วมกันกำหนดเพื่อเป็นแนวปฏิบัติในการบริหารจัดการภัยทุจริต

5.2 หลักการ

ผู้ให้บริการที่เกี่ยวข้องกับการทำธุรกรรมด้วยบัตร ได้แก่ ผู้ให้บริการออกบัตร ผู้ให้บริการรับบัตร และผู้ให้บริการระบบเครือข่ายบัตร ต้องให้ความสำคัญกับการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตรอย่างเหมาะสมและทันกาล โดยดำเนินการในแนวทางที่เป็นประโยชน์ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อช่วยป้องกันและลดความเสียหายที่จะเกิดขึ้นกับประชาชนอย่างมีประสิทธิผล โดยต้องสร้างความสมดุลระหว่างความสะดวกและความปลอดภัยในการทำธุรกรรมด้วยบัตร และคำนึงถึงการคุ้มครองผู้ใช้บริการอย่างเป็นธรรม

5.3 หลักเกณฑ์การบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตร

5.3.1 ด้านธรรมาภิบาลและการกำหนดนโยบาย

คณะกรรมการและผู้บริหารระดับสูงสุดของผู้ให้บริการออกบัตรต้องกำกับดูแลให้ผู้ให้บริการออกบัตรมีการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตร ที่เหมาะสมกับรูปแบบและผลกระทบของภัยทุจริตที่เกิดขึ้น และมีการแก้ไขสถานการณ์ที่ทันกาล เพื่อป้องกันและลดความเสียหายที่จะเกิดขึ้นกับผู้ใช้บริการตั้งแต่ต้นจนจบกระบวนการ (end-to-end) เริ่มตั้งแต่การป้องกัน การติดตามและตรวจจับธุรกรรม การจัดการและแก้ไขสถานการณ์เมื่อเกิดเหตุภัยทุจริต การดูแลผู้ใช้บริการที่ได้รับผลกระทบ และความร่วมมือกับผู้ที่เกี่ยวข้อง โดยกำหนดให้เป็นความเสี่ยงสำคัญที่ผู้ให้บริการออกบัตรต้องมีการบริหารจัดการแบบบูรณาการ ซึ่งผู้ให้บริการออกบัตรต้องดำเนินการ ดังนี้

(1) กำหนดให้มีคณะทำงานหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย ทำหน้าที่กำหนดนโยบายและกำกับดูแลการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตร อย่างชัดเจน เพื่อให้องค์กรให้ความสำคัญและมีแนวทางบริหารจัดการภัยทุจริตที่เหมาะสม ทันกาล และมีประสิทธิผลอย่างต่อเนื่อง สอดรับกับบริบทของปัญหาภัยทุจริตในแต่ละช่วงเวลา และสามารถลดความเสียหายที่จะเกิดขึ้นกับประชาชนได้ทันท่วงที

(2) กำหนดนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตรที่ชัดเจนเป็นลายลักษณ์อักษร ซึ่งได้รับความเห็นชอบจากคณะกรรมการของผู้ให้บริการออกบัตร และจัดให้มีการทบทวนและปรับปรุงนโยบายอย่างสม่ำเสมอโดยเฉพาะเมื่อมีเหตุการณ์หรือการเปลี่ยนแปลงที่ส่งผลกระทบต่อประสิทธิผลของการบริหารจัดการภัยทุจริตอย่างมีนัยสำคัญหรือตามความถี่ที่เหมาะสม รวมทั้งมีการเผยแพร่และสื่อสารแก่บุคลากรทุกระดับในองค์กรเพื่อให้สามารถปฏิบัติตามได้อย่างถูกต้องและเหมาะสม โดยนโยบายดังกล่าวต้องสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง และบริบทของปัญหาภัยทุจริตในแต่ละช่วงเวลา ครอบคลุมอย่างน้อย ดังนี้

(2.1) **บทบาทหน้าที่ของคณะทำงานหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย** และหน่วยงานที่รับผิดชอบ เพื่อผลักดันให้มีการบริหารจัดการภัยทุจริตที่มีประสิทธิผล รวมทั้งประเมินความพร้อมขององค์กรทั้งในด้านบุคลากร กระบวนการ เทคโนโลยีและเครื่องมือที่ใช้ในการบริหารจัดการภัยทุจริตอย่างสม่ำเสมอ

(2.2) **แนวทางและกระบวนการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตร**ตั้งแต่ต้นจนจบกระบวนการ (end-to-end) โดยเริ่มตั้งแต่การป้องกัน การติดตามและตรวจจับธุรกรรม การจัดการและแก้ไขสถานการณ์เมื่อเกิดเหตุภัยทุจริต การดูแลผู้ใช้บริการที่ได้รับผลกระทบ และความร่วมมือกับผู้ที่เกี่ยวข้อง เพื่อให้การบริหารจัดการภัยทุจริตเป็นไปอย่างมีประสิทธิผล

(2.3) **การติดตามและวัดประสิทธิผล**ของการบริหารจัดการภัยทุจริตอย่างต่อเนื่อง เพื่อทบทวนแนวทางและกระบวนการให้เหมาะสมกับสถานการณ์อยู่เสมอ

(3) กำหนดเป้าหมายและตัวชี้วัดในการประเมินประสิทธิผลของการบริหารจัดการภัยทุจริตที่ชัดเจนและวัดผลได้จริง และต้องปรับปรุงอย่างสม่ำเสมอให้สอดคล้องกับสถานการณ์และรูปแบบภัยทุจริต เช่น สัดส่วนรายการธุรกรรมทุจริตทั้งที่ตรวจพบเองและได้รับแจ้งจากผู้ใช้บริการหรือหน่วยงานภายนอก สัดส่วนจำนวนบัตรที่พบปัญหาภัยทุจริต จำนวนข้อร้องเรียนของผู้ใช้บริการ และระยะเวลาเฉลี่ยในการแก้ไขปัญหาให้ผู้ใช้บริการ

(4) จัดให้มีบุคลากร กระบวนการ เทคโนโลยีและเครื่องมือที่ใช้ในการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตรอย่างเพียงพอและเหมาะสม โดยในการออกแบบและพัฒนาระบบงาน กระบวนการ และผลิตภัณฑ์ ต้องคำนึงถึงเหตุการณ์และปัจจัยความเสี่ยงที่อาจทำให้เกิดภัยทุจริตด้วย เช่น การยืนยันตัวตนที่สอดคล้องกับช่องทางการใช้งานเพื่อป้องกันการถูกผู้ไม่ประสงค์ดีทำธุรกรรมโดยไม่ได้รับอนุญาตแทนผู้ใช้บริการตัวจริง และการติดตามและตรวจจับธุรกรรมผิดปกติที่สอดคล้องกับระดับความเสี่ยงของธุรกรรมและรูปแบบของภัยทุจริต เพื่อป้องกันและจำกัดความเสียหายที่จะเกิดขึ้น

นอกจากนี้ ผู้ให้บริการออกบัตรต้องสื่อสารและพัฒนาองค์ความรู้ของบุคลากรทุกระดับในองค์กรเกี่ยวกับการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตรอย่างต่อเนื่อง เพื่อให้มีความรู้ความเข้าใจที่เพียงพอในการกำกับดูแล บริหารจัดการและรับมือกับภัยทุจริตรูปแบบใหม่ ๆ ที่อาจเกิดขึ้น

(5) ติดตามและประเมินประสิทธิผลของการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตร รวมทั้งปรับปรุงระบบงาน กระบวนการ และผลิตภัณฑ์ ให้สอดคล้องกับผล

การประเมินและรูปแบบของภัยทุจริต เพื่อให้สามารถตรวจจับและจัดการธุรกรรมที่ผิดปกติหรืออาจเข้าข่ายการทำทุจริตได้ทันท่วงที โดยผู้บริหารระดับสูงสุด คณะทำงานหรือผู้บริหารระดับสูงที่ได้รับมอบหมายต้องจัดให้มีการรายงานประเด็นที่มีนัยสำคัญต่อคณะกรรมการของผู้ให้บริการออกบัตรอย่างต่อเนื่อง

นอกจากนี้ หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง หน่วยงานที่ทำหน้าที่กำกับการปฏิบัติตามกฎเกณฑ์ และหน่วยงานที่ทำหน้าที่ตรวจสอบภายใน ต้องมีส่วนร่วมในการผลักดันให้องค์กรมีกระบวนการควบคุมดูแลความเสี่ยงที่ดี เพื่อให้การบริหารจัดการภัยทุจริตขององค์กรดำเนินการได้อย่างเหมาะสมและทันกาล

(6) สนับสนุนการจัดทำมาตรฐานอุตสาหกรรม โดยให้ครอบคลุมกระบวนการบริหารจัดการภัยทุจริตที่จำเป็นและสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง เพื่อให้มั่นใจว่ากระบวนการบริหารจัดการภัยทุจริตมีมาตรฐานเดียวกัน

5.3.2 ด้านการบริหารจัดการภัยทุจริต

ผู้ให้บริการออกบัตร ผู้ให้บริการรับบัตรและผู้ให้บริการระบบเครือข่ายบัตร ต้องจัดให้มีกรอบการดำเนินการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตรที่ชัดเจน เริ่มตั้งแต่การสมัครหรือเปิดใช้บริการ การทำธุรกรรมด้วยบัตร การจัดการและแก้ไขสถานการณ์เมื่อเกิดเหตุภัยทุจริต การดูแลผู้ใช้บริการ จนสิ้นสุดการให้บริการหรือยุติความสัมพันธ์กับผู้ใช้บริการ โดยต้องดำเนินการอย่างน้อย ดังนี้

(1) การรู้จักผู้ใช้บริการ (Know Your Customer: KYC) และการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับผู้ใช้บริการ (Customer Due Diligence: CDD)

ผู้ให้บริการออกบัตรต้องมีกระบวนการและดำเนินการรู้จักผู้ใช้บริการ (KYC) สำหรับการเปิดใช้บริการบัตร ทั้งในการแสดงตนของผู้ใช้บริการ (Identification) และการพิสูจน์ตัวตนผู้ใช้บริการ (Verification) จากแหล่งข้อมูลที่น่าเชื่อถือ เพื่อตรวจสอบให้มั่นใจว่าข้อมูลและหลักฐานการแสดงตนที่ได้รับจากผู้ใช้บริการมีความถูกต้อง ความแท้จริง และความเป็นปัจจุบัน รวมถึงพิสูจน์ได้ว่าผู้ใช้บริการเป็นเจ้าของข้อมูลและหลักฐานดังกล่าวจริง และต้องมีกระบวนการและดำเนินการประเมินความเสี่ยงผู้ใช้บริการและตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับผู้ใช้บริการ (CDD) เมื่อเริ่มทำธุรกรรมครั้งแรกและตรวจสอบเป็นระยะจนสิ้นสุดการให้บริการหรือยุติความสัมพันธ์กับผู้ใช้บริการ ซึ่งหากพบว่าผู้ใช้บริการบัตรมีเหตุหรือพฤติกรรมอันควรสงสัยหรือสุ่มเสี่ยงต่อการนำบัตรไปใช้เป็นเครื่องมือในการกระทำความผิดหรือทุจริต เช่น พฤติกรรมการใช้งานบัตรที่ไม่สอดคล้องกับข้อมูลของผู้ใช้บริการ ผู้ให้บริการออกบัตรต้องยกระดับการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับผู้ใช้บริการในระดับเข้มข้น (Enhanced Customer Due Diligence: EDD) โดยตรวจสอบข้อมูลอื่นเพิ่มเติม เช่น แหล่งที่มาของ

เงินหรือทรัพย์สิน และแหล่งที่มาของฐานะความมั่งคั่ง ทั้งนี้ ให้ถือปฏิบัติตามหลักเกณฑ์ของกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และประกาศธนาคารแห่งประเทศไทยที่เกี่ยวข้อง เช่น ประกาศหลักเกณฑ์การรู้จักลูกค้า (KYC) สำหรับการเปิดบัญชีเงินฝาก และประกาศหลักเกณฑ์การรู้จักลูกค้า (KYC) สำหรับการเปิดใช้บริการเงินอิเล็กทรอนิกส์ รวมถึงกฎหมาย ประกาศและหลักเกณฑ์อื่นที่เกี่ยวข้อง

(2) การติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมด้วยบัตร (monitoring and detection)

ผู้ให้บริการออกบัตรต้องมีกระบวนการและดำเนินการติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมด้วยบัตรที่มีประสิทธิผลและเป็นลักษณะเชิงรุก ครอบคลุมรูปแบบของภัยทุจริตที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง ทั้งในลักษณะที่ผู้ใช้บริการไม่ได้ทำธุรกรรมด้วยตนเองหรือถูกสวมรอยทำธุรกรรมแทนตนเอง (unauthorized payment fraud) และลักษณะที่ผู้ใช้บริการถูกหลอกลวงให้หลงเชื่อและทำธุรกรรมให้มิจฉาชีพด้วยตนเอง (authorized payment fraud) โดยต้องสามารถประเมินและจัดระดับความเสี่ยงของธุรกรรมด้วยบัตรแต่ละประเภท รวมถึงตรวจจับธุรกรรมที่มีความผิดปกติได้อย่างทันท่วงที เพื่อให้มีการจัดการธุรกรรมที่ผิดปกติหรืออาจเข้าข่ายการทำทุจริตที่เหมาะสมและทันกาล ซึ่งจะช่วยจำกัดความเสียหายและป้องกันไม่ให้ขยายตัวหรือลุกลามเป็นวงกว้าง โดยอย่างน้อยต้องดำเนินการ ดังนี้

(2.1) **จัดให้มีระบบการติดตามและตรวจจับรายการธุรกรรมผิดปกติหรืออาจเข้าข่ายการทำทุจริต**จากการทำธุรกรรมด้วยบัตรที่สามารถตรวจจับได้อย่างทันท่วงที และต่อเนื่องทั้งในและนอกเวลาทำการ (24x7) โดยควรนำระบบวิเคราะห์ข้อมูล (data analytics) หรือเทคโนโลยีปัญญาประดิษฐ์ (artificial intelligence) มาใช้ เพื่อให้สามารถติดตามและตรวจจับความผิดปกติได้ดียิ่งขึ้น และเท่าทันกับสถานการณ์และรูปแบบภัยทุจริตใหม่ ๆ อันจะช่วยให้ผู้ให้บริการออกบัตรสามารถระงับเหตุการณ์ภัยทุจริตดิจิทัลและป้องกันความเสียหายที่อาจเกิดขึ้นได้อย่างทันกาล

(2.2) **จัดให้มีการประเมินและจัดระดับความเสี่ยงของธุรกรรมแต่ละประเภท ตามลักษณะผลิตภัณฑ์ ช่องทางการให้บริการ พฤติกรรมการใช้งาน และรูปแบบภัยทุจริต** เช่น ธุรกรรมการชำระเงินครั้งแรก ธุรกรรมการชำระเงินผ่านช่องทางออนไลน์ ธุรกรรมการชำระเงินด้วยวิธี contactless ธุรกรรมการชำระเงินในต่างประเทศ ธุรกรรมการชำระด้วยเงินตราต่างประเทศ ธุรกรรมการชำระเงินมูลค่าต่ำที่มีความถี่สูง ธุรกรรมการถอนเงินสด ธุรกรรมการเบิกถอนวงเงินสินเชื่อบัตรเครดิต และธุรกรรมการชำระเงินคืนบัตรเครดิตที่ทำให้สามารถใช้จ่ายได้สูงกว่าวงเงินสินเชื่อที่ได้รับ

(2.3) **กำหนดเงื่อนไขการตรวจจับ**รายการธุรกรรมที่มีความผิดปกติหรืออาจเข้าข่ายการทำทุจริตให้สอดคล้องกับระดับความเสี่ยงของธุรกรรม และทบทวนและปรับปรุงเงื่อนไขการตรวจจับอย่างสม่ำเสมอ

(3) การจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตร (actions)

ผู้ให้บริการออกบัตรต้องมีกระบวนการและดำเนินการป้องกัน จำกัดและระงับความเสียหายจากภัยทุจริตจากการทำธุรกรรมด้วยบัตรอย่างรวดเร็ว เพียงพอและเหมาะสม สอดคล้องตามระดับความเสี่ยงของธุรกรรม ซึ่งประกอบด้วยการป้องกันและจำกัดความเสียหายให้แก่ผู้ใช้บริการจากภัยทุจริต และการจัดการบัตรที่มีความเสี่ยงที่อาจถูกใช้ในการกระทำความผิดของมิจฉาชีพและบัตรที่มีรายชื่อผู้ใช้บริการเป็นเจ้าของบัญชีม้า โดยอย่างน้อยต้องดำเนินการ ดังนี้

(3.1) การป้องกันและจำกัดความเสียหาย

ผู้ให้บริการออกบัตรต้องจัดให้มีกระบวนการและดำเนินการป้องกันและจำกัดความเสียหายให้แก่ผู้ใช้บริการที่เพียงพอและเหมาะสม สอดคล้องกับระดับความเสี่ยงของการทำธุรกรรมตามลักษณะผลิตภัณฑ์ ช่องทางการให้บริการ พฤติกรรมการใช้งาน และรูปแบบภัยทุจริต เช่น การยกระดับการยืนยันตัวตนผู้ใช้บริการที่รัดกุม การให้ผู้ใช้บริการสามารถบริหารจัดการความเสี่ยงในการใช้บริการบัตรที่เหมาะสมกับตนเอง การแจ้งเตือนเมื่อมีการทำธุรกรรมด้วยบัตร และการตรวจสอบการทำธุรกรรมกับผู้ใช้บริการเมื่อพบความผิดปกติ เพื่อลดความเสียหายให้แก่ผู้ใช้บริการจากการถูกหลอกลวงจากมิจฉาชีพหรือการถูกนำบัตรมาใช้เป็นเครื่องมือในการกระทำความผิดหรือทุจริต

(3.1.1) **จัดให้มีการยืนยันตัวตนผู้ใช้บริการในการทำธุรกรรมที่เกี่ยวข้องกับบัตร**ทั้งในลักษณะที่มีการแสดงบัตร (card present) และการใช้ข้อมูลบัตรโดยไม่ต้องแสดงบัตร (card not present) ด้วยวิธีการที่มีความปลอดภัยสูง เท่าทันกับภัยทุจริตที่เกิดขึ้น และเป็นไปตามมาตรฐานสากล โดยใช้การยืนยันตัวตนแบบหลายวิธี (multi-factor authentication) ตามระดับความเสี่ยงของธุรกรรม เว้นแต่การทำธุรกรรมที่มีความเสี่ยงต่ำควรดำเนินการที่สอดคล้องตามมาตรฐานหรือแนวทางที่ได้รับการยอมรับโดยทั่วไป ซึ่งวิธีการยืนยันตัวตนอาจใช้เป็นรหัสส่วนบุคคล (personal identification number: PIN) หรือรหัสใช้ครั้งเดียว (one-time password: OTP) หรือการยืนยันผ่านแอปพลิเคชันของผู้ให้บริการออกบัตร (in-application authentication) หรือข้อมูลชีวมิติ (biometrics) ของผู้ใช้บริการ เป็นต้น

สำหรับการใช้รหัสใช้ครั้งเดียว (OTP) ผู้ให้บริการออกบัตรต้องจัดให้มีรูปแบบข้อมูล OTP ที่แสดงถึงรายละเอียดการทำธุรกรรมอย่างชัดเจน โดยเรียงลำดับจากจำนวนเงิน สกุลเงิน รหัส OTP ชื่อร้านค้า และหมายเลขอ้างอิงธุรกรรม เพื่อให้ผู้ใช้บริการสามารถ

ตรวจสอบความถูกต้องของรายการธุรกรรมและข้อมูล OTP ก่อนดำเนินการยืนยันการทำธุรกรรม อีกทั้งผู้ให้บริการออกบัตรต้องสร้างความตระหนักรู้และแจ้งเตือนให้ผู้ใช้บริการตรวจสอบแหล่งที่มาของข้อมูล OTP และไม่เปิดเผยรหัส OTP ให้แก่บุคคลอื่น เพื่อช่วยป้องกันภัยทุจริตจากการถูกหลอกลวง

ทั้งนี้ สำหรับการให้บริการบัตรเครดิต ผู้ให้บริการออกบัตร ผู้ให้บริการรับบัตรและผู้ให้บริการระบบเครือข่ายบัตร ต้องร่วมกันสนับสนุนและผลักดันให้เกิดการยกระดับการยืนยันตัวตนผู้ใช้บริการด้วยวิธีการใช้ข้อมูลจากชิปการ์ดร่วมกับรหัสส่วนบุคคล (chip and PIN) สำหรับการทำธุรกรรมในลักษณะที่มีการแสดงบัตร (card present) เพื่อช่วยป้องกันภัยทุจริต และสร้างให้เกิดความปลอดภัยในการทำธุรกรรมด้วยบัตร

(3.1.2) **จัดให้มีระบบหรือช่องทางรองรับให้ผู้ใช้บริการสามารถบริหารจัดการความเสี่ยงในการทำธุรกรรมด้วยบัตรได้ด้วยตนเอง** เช่น แอปพลิเคชันของผู้ให้บริการออกบัตร โดยต้องมีการยืนยันตัวตนผู้ใช้บริการตามข้อ (3.1.1) ทุกครั้งก่อนดำเนินการ เพื่อให้มั่นใจว่าผู้ใช้บริการเป็นผู้ดำเนินการด้วยตนเอง อย่างน้อยครอบคลุม

(3.1.2.1) การตั้งค่าเปิด-ปิด และกำหนดวงเงิน ในการทำธุรกรรมการชำระเงินผ่านช่องทางออนไลน์ การทำธุรกรรมการชำระเงินด้วยวิธี contactless และการทำธุรกรรมการชำระเงินในต่างประเทศ โดยต้องตั้งค่าเริ่มต้นเป็นปิดหรือกำหนดวงเงินสูงสุดต่อรายการเป็นศูนย์ ของการทำธุรกรรมดังกล่าว ทั้งนี้ ผู้ให้บริการออกบัตรอาจกำหนดให้ผู้ใช้บริการสามารถเลือกเปิดการทำธุรกรรมดังกล่าว ไปพร้อมกับการเปิดใช้งานบัตรในครั้งแรกด้วยก็ได้

(3.1.2.2) การปรับเพิ่มหรือลดวงเงินสูงสุดต่อครั้งหรือต่อวันของการทำธุรกรรมแต่ละประเภท

(3.1.2.3) การระงับการใช้บัตรเป็นการชั่วคราว และการยกเลิกการระงับการใช้บัตรเพื่อให้กลับมาใช้งานได้ตามปกติ

(3.1.2.4) การอายัดบัตร

(3.1.3) **จัดให้มีกระบวนการรองรับให้ผู้ใช้บริการสามารถแจ้งความประสงค์ขอปรับลดวงเงินสินเชื่อบัตรเครดิต ผ่านช่องทางที่ผู้ใช้บริการสามารถติดต่อผู้ให้บริการออกบัตรได้อย่างสะดวกและรวดเร็ว หรือช่องทางที่ผู้ให้บริการออกบัตรติดต่อกับผู้ใช้บริการ** โดยเพิ่มเติมจากการให้บริการผ่านศูนย์บริการ (call center) อย่างน้อย 1 ช่องทาง เช่น แอปพลิเคชันของผู้ให้บริการออกบัตร บัญชีทางการบนแพลตฟอร์มส่งข้อความ (เช่น LINE Official Account) ข้อความสั้น (SMS) และอีเมล ซึ่งต้องมีการยืนยันตัวตนผู้ใช้บริการตามข้อ (3.1.1) ทุกครั้งก่อนดำเนินการ เพื่อให้

มั่นใจว่าผู้ใช้บริการเป็นผู้ดำเนินการด้วยตนเอง ทั้งนี้ ผู้ให้บริการออกบัตรต้องเร่งดำเนินการให้แล้วเสร็จโดยเร็วนับจากวันที่ได้รับแจ้งความประสงค์จากผู้ใช้บริการ

(3.1.4) **จัดให้มีการแจ้งเตือนผู้ใช้บริการโดยทันที เมื่อมีการทำธุรกรรม โดยไม่เรียกเก็บค่าใช้จ่าย ผ่านช่องทางใดช่องทางหนึ่ง** เช่น แอปพลิเคชันของผู้ให้บริการออกบัตร บัญชีทางการบนแพลตฟอร์มส่งข้อความ (เช่น LINE Official Account) ข้อความสั้น (SMS) และอีเมล

(3.1.5) **จัดให้มีกระบวนการตรวจสอบการทำธุรกรรมกับผู้ใช้บริการโดยเร็ว เมื่อตรวจพบลักษณะหรือพฤติกรรมการใช้งานที่ผิดปกติ** ทั้งธุรกรรมที่ผู้ใช้บริการทำด้วยตนเอง (authorized payment) และธุรกรรมที่ผู้ใช้บริการอาจไม่ได้ทำด้วยตนเอง (unauthorized payment) เช่น การชะลอธุรกรรมและสอบถามผู้ใช้บริการก่อนการอนุมัติการทำธุรกรรม และการยับยั้งธุรกรรมเมื่อสอบถามผู้ใช้บริการและทราบว่าผู้ใช้บริการไม่ได้ทำธุรกรรมนั้น

(3.1.6) **จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลระหว่างการรับส่ง จัดเก็บหรือใช้ข้อมูลบัตร ที่สอดคล้องตามมาตรฐานสากล** เช่น มาตรฐาน The Payment Card Industry Data Security Standard (PCI DSS) รวมทั้งอาจนำเทคโนโลยีหรือวิธีการใหม่ ๆ มาใช้เพื่อยกระดับการรักษาความปลอดภัยในการทำธุรกรรม เช่น การใช้เทคโนโลยีสร้างเลขอ้างอิงเลขที่บัตร (tokenization)

สำหรับการให้บริการบัตรเอทีเอ็ม ให้ปฏิบัติตามหลักเกณฑ์ข้อ (3.1.1) และข้อ (3.1.4)

(3.2) การจัดการบัตรที่มีความเสี่ยงที่อาจถูกใช้ในการกระทำความผิดและบัตรที่มีรายชื่อผู้ใช้บริการเป็นเจ้าของบัญชีม้า

ผู้ให้บริการออกบัตรต้องมีกระบวนการและดำเนินการ จำกัดและระงับความเสียหายที่เกิดขึ้นจากบัตร ให้สอดคล้องตามระดับความเสี่ยงที่อาจถูกใช้เป็นเครื่องมือในกระทำความผิดของมิจฉาชีพ ได้อย่างเหมาะสมและทันกาล เช่น การลดวงเงินสินเชื่อบัตรเครดิต การควบคุมการใช้งาน การระงับการใช้งานเฉพาะบัตร การระงับการใช้งานบัตรทุกใบของผู้ใช้บริการ การยกเลิกการให้บริการบัตรกับผู้ใช้บริการ และการปฏิเสธการเปิดบัตรใหม่ รวมทั้งจัดการบัตรที่มีรายชื่อผู้ใช้บริการเป็นเจ้าของบัญชีม้า โดยให้ถือปฏิบัติตามประกาศและหลักเกณฑ์ของธนาคารแห่งประเทศไทยที่เกี่ยวข้องเป็นขั้นต่ำ

(4) การแก้ไขสถานการณ์และการดูแลผู้ใช้บริการ (response)

ผู้ให้บริการออกบัตรต้องกำหนดกระบวนการและดำเนินการแก้ไขสถานการณ์และดูแลผู้ใช้บริการ เมื่อผู้ใช้บริการเกิดปัญหาหรือเหตุการณ์ภัยทุจริตที่อาจก่อให้เกิดความเสียหายจากการทำธุรกรรมด้วยบัตร ตั้งแต่การจัดให้มีช่องทางติดต่อ การช่วยเหลือดูแลผู้ใช้บริการ และการรายงานเหตุการณ์ภัยทุจริตและการสื่อสารต่อสาธารณชน ที่ชัดเจน โปร่งใส รวดเร็ว และเป็นธรรม ให้ครอบคลุมทั้งกรณีที่ผู้ใช้บริการไม่ได้ทำธุรกรรมด้วยตนเอง (unauthorized payment fraud) และกรณีที่ผู้ใช้บริการถูกหลอกลวงให้ทำธุรกรรมด้วยตนเอง (authorized payment fraud) โดยอย่างน้อยต้องดำเนินการ ดังนี้

(4.1) การมีช่องทางติดต่อผู้ให้บริการ

ผู้ให้บริการออกบัตรต้องจัดให้มีช่องทางติดต่อเร่งด่วน (hotline) ทางโทรศัพท์ หรือวิธีการทางอิเล็กทรอนิกส์ที่ผู้ใช้บริการสามารถติดต่อเจ้าหน้าที่ของผู้ให้บริการออกบัตรเพื่อขอข้อมูล แจ้งเหตุภัยทุจริต และขอความช่วยเหลือ ได้อย่างเพียงพอ สะดวก รวดเร็ว และต่อเนื่องทั้งในและนอกเวลาทำการ (24x7) ทั้งนี้ หลังได้รับแจ้งเหตุ ผู้ให้บริการออกบัตรต้องเร่งดำเนินการช่วยเหลือและดูแลผู้ใช้บริการตามกระบวนการที่กำหนดโดยเป็นไปตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเคร่งครัด

(4.2) การช่วยเหลือและดูแลผู้ใช้บริการ

ผู้ให้บริการออกบัตรต้องมีกระบวนการและดำเนินการช่วยเหลือและดูแลผู้ใช้บริการ และกำหนดระยะเวลาและข้อตกลง (Service Level Agreement) ในการใช้บริการอย่างเหมาะสม ชัดเจน โปร่งใส รวดเร็ว และเป็นธรรม และดำเนินการช่วยเหลืออย่างเต็มที่โดยคำนึงถึงสิทธิและประโยชน์ที่ผู้ใช้บริการควรได้รับ เพื่อดูแลผู้ใช้บริการที่ได้รับความเสียหายหรือผลกระทบจากปัญหาหรือเหตุภัยทุจริตจากการทำธุรกรรมด้วยบัตร ครอบคลุมตั้งแต่การรับแจ้งปัญหาหรือเหตุภัยทุจริต การดำเนินการจัดการและแก้ไขปัญหา การประสานงานกับผู้ที่เกี่ยวข้อง การแจ้งความคืบหน้า การตรวจสอบและพิสูจน์ข้อเท็จจริง การแจ้งผลการตรวจสอบ และการเยียวยาหรือชดเชยความเสียหาย

(4.2.1) **จัดให้มีทีมงานที่มีความเชี่ยวชาญในการรับมือกับเหตุภัยทุจริต และเข้าใจกระบวนการดูแลผู้ใช้บริการที่ได้รับความเสียหายหรือผลกระทบจากเหตุภัยทุจริต** เพื่อให้ข้อมูล คำอธิบายและคำแนะนำแก่ผู้ใช้บริการได้อย่างถูกต้องและชัดเจน เช่น การปฏิเสธและการโต้แย้งรายการธุรกรรม การตรวจสอบและพิสูจน์ข้อเท็จจริง ข้อมูลและเอกสารหลักฐานที่ต้องจัดเตรียมเพื่อใช้ในการตรวจสอบและพิสูจน์ข้อเท็จจริง การประสานงานกับผู้ที่เกี่ยวข้องในการ

ช่วยเหลือและดูแลผู้ใช้บริการ การเยียวยาหรือชดเชยความเสียหาย และระยะเวลาดำเนินการในแต่ละขั้นตอน

(4.2.2) **จัดให้มีกระบวนการ ขั้นตอนหรือคู่มือการปฏิบัติงานในการช่วยเหลือและดูแลผู้ใช้บริการที่ชัดเจนและครบถ้วน** และดำเนินการอย่างเต็มที่โดยคำนึงถึงสิทธิและประโยชน์ที่ผู้ใช้บริการควรได้รับ ครอบคลุมตั้งแต่การรับแจ้งปัญหาหรือเหตุภัยทุจริต การดำเนินการจัดการและแก้ไขปัญหา การประสานงานกับผู้ที่เกี่ยวข้อง การแจ้งความคืบหน้า การตรวจสอบและพิสูจน์ข้อเท็จจริง การแจ้งผลการตรวจสอบ และการเยียวยาหรือชดเชยความเสียหาย รวมทั้งกำหนดระยะเวลาดำเนินการในแต่ละขั้นตอนที่เหมาะสม เพื่อเป็นมาตรฐานการปฏิบัติงานในการดูแลและให้ความช่วยเหลือผู้ใช้บริการ เช่น ผู้ให้บริการออกบัตรต้องรับแจ้งปัญหาหรือเหตุภัยทุจริตภายใน 1 วันนับจากเวลาที่ผู้ใช้บริการได้ติดต่อผู้ให้บริการออกบัตร ซึ่งผู้ให้บริการออกบัตรต้องให้ข้อมูล คำอธิบายและคำแนะนำตามข้อ (4.2.1) แก่ผู้ใช้บริการอย่างถูกต้องและชัดเจนด้วย

(4.2.3) **จัดให้มีการประสานงานกับผู้ที่เกี่ยวข้อง** เช่น ผู้ให้บริการรับบัตรและผู้ให้บริการระบบเครือข่ายบัตร ในการช่วยเหลือและดูแลผู้ใช้บริการโดยทันทีอย่างเต็มความสามารถ เพื่อระงับหรือจำกัดหรือหยุดความเสียหายหรือผลกระทบจากปัญหาหรือเหตุภัยทุจริต และในกรณีที่จำเป็นต้องประสานงานไปยังร้านค้าเพื่อให้ยกเลิกรายการธุรกรรม ผู้ให้บริการรับบัตรต้องให้ความร่วมมือในการประสานงานกับร้านค้าโดยทันที

(4.2.4) **จัดให้มีการสื่อสารและทำความเข้าใจกับผู้ใช้บริการอย่างต่อเนื่องเป็นระยะ** ตั้งแต่การรับแจ้งปัญหาหรือเหตุภัยทุจริตจากผู้ใช้บริการจนสิ้นสุดกระบวนการดูแลผู้ใช้บริการ รวมถึงการที่ผู้ใช้บริการอาจต้องรับผิดชอบในความเสียหายด้วย เพื่อให้ผู้ใช้บริการทราบกระบวนการช่วยเหลือดูแลและข้อมูลสำคัญได้อย่างชัดเจนและครบถ้วน และสามารถติดตามความคืบหน้าและสถานะการดำเนินการของการแก้ไขปัญหาและให้ความช่วยเหลือ เช่น ในระหว่างที่ผู้ให้บริการออกบัตรตรวจสอบและพิสูจน์ข้อเท็จจริง และประสานงานกับผู้ที่เกี่ยวข้อง ผู้ให้บริการออกบัตรต้องติดต่อและแจ้งให้ผู้ใช้บริการทราบความคืบหน้าและการดำเนินการถัดไปให้ชัดเจน

(4.2.5) **จัดให้มีกระบวนการตรวจสอบและพิสูจน์ข้อเท็จจริงของเหตุที่ได้รับแจ้งจากผู้ใช้บริการ (investigate process)** ซึ่งต้องมีขั้นตอนและระยะเวลาการดำเนินการที่ละเอียด ชัดเจน โปร่งใส และเป็นธรรมกับผู้ใช้บริการ โดยคำนึงถึงสิทธิและประโยชน์ที่ผู้ใช้บริการควรได้รับ และต้องดำเนินการให้เป็นไปตามระยะเวลาที่กำหนดและได้แจ้งให้ผู้ใช้บริการทราบ

ในกรณีบัตรเครดิต เมื่อผู้ให้บริการออกบัตรได้รับแจ้งปัญหาหรือเหตุภัยทุจริตจากผู้ใช้บริการแล้ว ผู้ให้บริการออกบัตรต้องดำเนินการตั้งพักยอด (suspend) รายการธุรกรรมที่ได้รับแจ้งไว้ก่อน พร้อมแสดงสถานะการตั้งพักยอดไว้ในใบรายการเดินบัญชีบัตรเครดิต (statement) ให้ชัดเจน โดยถือว่าผู้ให้บริการออกบัตรยังไม่มีสิทธิ์เรียกร้องให้ชำระเงินในรายการธุรกรรมนั้น

(4.2.6) **จัดให้มีการแจ้งผลการตรวจสอบและพิสูจน์ข้อเท็จจริงให้ผู้ใช้บริการทราบ**อย่างชัดเจนและครบถ้วน **และดำเนินการชดเชยความเสียหายหรือแจ้งให้ผู้ใช้บริการมีส่วนร่วมรับผิดชอบในความเสียหาย** ดังนี้

(4.2.6.1) หากตรวจสอบและพิสูจน์แล้วมีเหตุอันเชื่อได้ว่าไม่ได้เกิดจากความผิดของผู้ใช้บริการ หรือผู้ใช้บริการไม่มีส่วนเกี่ยวข้อง ซึ่งผู้ใช้บริการไม่ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น เช่น กรณีผู้ใช้บริการไม่ได้ทำธุรกรรมด้วยตนเองหรือถูกสวมรอยทำธุรกรรมแทนตนเอง (unauthorized payment fraud) และเป็นผู้สุจริตที่ไม่ได้ประมาทเลินเล่อหรือขาดความระมัดระวังตามสมควรในการใช้บัตร ผู้ให้บริการออกบัตรต้องเยียวยาความเสียหายให้แก่ผู้ใช้บริการ ดังนี้

(1) กรณีบัตรเดบิต บัตรเอทีเอ็ม หรือบัตรเงินอิเล็กทรอนิกส์ที่ใช้บริการผ่านระบบเครือข่ายบัตร ให้คืนเงินตามยอดที่ถูกตัดชำระให้แก่ผู้ใช้บริการโดยเร็วภายใน 5 วันนับแต่วันที่ผู้ให้บริการออกบัตรตรวจสอบและพิสูจน์แล้วมีเหตุอันเชื่อได้ว่าไม่ได้เกิดจากความผิดของผู้ใช้บริการ หรือผู้ใช้บริการไม่มีส่วนเกี่ยวข้อง

(2) กรณีบัตรเครดิต ให้ยกเลิกการเรียกชำระเงินในรายการธุรกรรมนั้น โดยผู้ใช้บริการไม่ต้องชำระเงินและค่าใช้จ่ายอื่น ๆ เช่น ดอกเบี้ย ที่เกิดขึ้นจากธุรกรรมดังกล่าว

(4.2.6.2) หากตรวจสอบและพิสูจน์แล้วมีเหตุอันเชื่อได้ว่าเกิดจากความผิดของผู้ใช้บริการ หรือผู้ใช้บริการมีส่วนเกี่ยวข้อง ซึ่งผู้ใช้บริการอาจต้องมีส่วนร่วมรับผิดชอบต่อความเสียหายที่เกิดขึ้น เช่น ผู้ใช้บริการประมาทเลินเล่อหรือขาดความระมัดระวังตามสมควรในการใช้บัตร ผู้ใช้บริการมีส่วนเกี่ยวข้องในการทำรายการธุรกรรมหรือยืนยันรายการธุรกรรมด้วยตนเอง และผู้ใช้บริการไม่ได้แจ้งให้ผู้ให้บริการออกบัตรทราบโดยเร็วและสินค้าหรือบริการได้ถูกส่งออกจากร้านค้าหรือผู้ให้บริการแล้ว ผู้ให้บริการออกบัตรต้องชี้แจงให้ผู้ใช้บริการทราบถึงเหตุผลและข้อสรุปของการเรียกชำระเงิน และแจ้งรายละเอียดของการเก็บเงินให้ชัดเจนและครบถ้วน รวมทั้งมีกลไกรองรับกรณีที่ผู้ใช้บริการไม่เห็นด้วยกับความเสียหายที่ผู้ให้บริการออกบัตรกำหนดให้รับผิดชอบ

(4.3) การรายงานเหตุการณ์ภัยทุจริตและการสื่อสารต่อสาธารณชน

ผู้ให้บริการออกบัตร ผู้ให้บริการรับบัตรและผู้ให้บริการระบบเครือข่ายบัตร ต้องมีกระบวนการและดำเนินการรายงานเหตุการณ์ภัยทุจริตจากการทำธุรกรรมด้วยบัตรแก่คณะกรรมการ หรือผู้บริหารระดับสูงสุด หรือคณะทำงานหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย ให้เหมาะสมตามระดับความรุนแรงของเหตุการณ์

นอกจากนี้ ในกรณีที่เกิดเหตุการณ์ภัยทุจริตจากการทำธุรกรรมด้วยบัตรกับผู้ให้บริการออกบัตร ผู้ให้บริการรับบัตรหรือผู้ให้บริการระบบเครือข่ายบัตร หลายรายพร้อมกัน ซึ่งส่งผลกระทบในวงกว้างต่อความเชื่อมั่นของระบบการเงินหรือระบบการชำระเงิน ผู้ให้บริการ สมาคมของผู้ให้บริการ และหน่วยงานอื่นที่เกี่ยวข้อง ควรร่วมกันสื่อสารเพื่อชี้แจงและทำความเข้าใจกับผู้ใช้บริการโดยเร็ว และกำหนดแนวทางการช่วยเหลือและดูแลผู้ใช้บริการให้เป็นมาตรฐานเดียวกัน

(5) การสร้างความตระหนักรู้ (awareness)

ผู้ให้บริการออกบัตรมีหน้าที่ในการสร้างความตระหนักรู้เกี่ยวกับภัยทุจริตจากการทำธุรกรรมด้วยบัตรให้แก่ผู้ใช้บริการ โดยต้องมีการสื่อสารและประชาสัมพันธ์ข้อมูลการใช้บริการที่สำคัญและภัยทุจริตเกี่ยวกับการทำธุรกรรมด้วยบัตร ในลักษณะเชิงรุกให้ผู้ใช้บริการทราบอย่างชัดเจนและต่อเนื่อง ผ่านช่องทางที่ผู้ใช้บริการสามารถเข้าถึงได้ง่าย เพื่อสร้างให้เกิดความเข้าใจและเพิ่มความระมัดระวังในการทำธุรกรรมด้วยบัตร ซึ่งจะช่วยป้องกันและลดโอกาสเกิดความเสียหายจากภัยทุจริต เช่น ข้อควรระมัดระวังในการใช้งานบัตร วิธีการบริหารจัดการความเสี่ยงด้วยตนเอง ขั้นตอนและแนวทางการจัดการเมื่อพบความผิดปกติหรือเกิดเหตุ และการให้ข้อมูลรูปแบบของภัยทุจริตที่เกิดขึ้นในปัจจุบันและวิธีการป้องกัน

(6) ความร่วมมือ (collaboration)

ผู้ให้บริการออกบัตร ผู้ให้บริการรับบัตรและผู้ให้บริการระบบเครือข่ายบัตร ต้องมีความร่วมมือระหว่างกันเพื่อส่งเสริมและสนับสนุนให้เกิดความปลอดภัยของการใช้งานบัตรและการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตรได้อย่างทันกาล สอดคล้องกับสภาพแวดล้อมของการให้บริการบัตร โดยอย่างน้อยต้องดำเนินการ ดังนี้

(6.1) ผู้ให้บริการออกบัตรและผู้ให้บริการรับบัตรต้องมีความร่วมมือระหว่างกันในด้านต่าง ๆ เพื่อส่งเสริมและสนับสนุนการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตรให้มีประสิทธิผลมากขึ้น เช่น การแลกเปลี่ยนข้อมูลและรูปแบบภัยทุจริตที่เกิดขึ้น และการ

กำหนดมาตรฐานการแก้ไขสถานการณ์และการดูแลผู้ใช้บริการ และต้องเปิดเผยหรือแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับเหตุการณ์ภัยทุจริตได้อย่างถูกต้องและรวดเร็ว ผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล ตามที่กำหนดไว้ในกฎหมายว่าด้วยมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี รวมถึงกฎหมาย ประกาศและหลักเกณฑ์อื่นที่เกี่ยวข้อง เพื่อให้สามารถร่วมกันบริหารจัดการภัยทุจริตได้อย่างทันกาล รวมทั้งต้องให้การสนับสนุนข้อมูลที่ต้องใช้ในการสืบสวนสอบสวนและติดตามหาผู้กระทำผิดให้แก่พนักงานสอบสวนที่ได้รับมอบหมายเมื่อถูกร้องขออย่างทันกาล โดยมีผู้รับผิดชอบและประสานงานที่ชัดเจน

(6.2) ผู้ให้บริการระบบเครือข่ายบัตรต้องมีมาตรการที่ชัดเจนและต่อเนื่องในการส่งเสริมและสนับสนุนให้เกิดความปลอดภัยในการทำธุรกรรมด้วยบัตร รวมทั้งให้สมาชิกเครือข่ายบัตรของตนสามารถบริหารจัดการภัยทุจริตตั้งแต่การออกบัตร การยืนยันตัวตน การติดตามและตรวจจับความผิดปกติ ตลอดจนการแก้ไขสถานการณ์และดูแลผู้ใช้บริการ อย่างน้อยครอบคลุม

(6.2.1) **กำหนดกฎเกณฑ์หรือข้อกำหนด (scheme rules) ที่ให้ความสำคัญกับการดูแลความเสี่ยงและการคุ้มครองผู้ใช้บริการเป็นสำคัญ** และกำหนดแผนงานที่ชัดเจนเพื่อให้สมาชิกเครือข่ายบัตรยกระดับความมั่นคงปลอดภัยและการบริหารจัดการความเสี่ยงจากการทำธุรกรรมด้วยบัตร โดยผู้ให้บริการระบบเครือข่ายบัตรต้องดูแลให้สมาชิกมีการปฏิบัติให้เป็นไปตามแผนงานที่กำหนดไว้ และทบทวนกฎเกณฑ์หรือข้อกำหนดและแผนงานอย่างสม่ำเสมอโดยให้สอดคล้องกับบริบทและสภาพแวดล้อมของการให้บริการในขณะนั้น

(6.2.2) **จัดให้มีระบบ ช่องทาง กลไก และผู้รับผิดชอบในการประสานงานและร่วมมือกับสมาชิกเครือข่ายบัตร** เพื่อช่วยเหลือและสนับสนุนข้อมูลที่เป็นประโยชน์ให้สมาชิกสามารถพัฒนาระบบการป้องกันและตรวจจับภัยทุจริต และมีกระบวนการตอบสนองและรับมือภัยทุจริต ได้อย่างเท่าทันและมีประสิทธิภาพยิ่งขึ้น รวมทั้งมีช่องทางในการติดตามธุรกรรมและช่วยเหลือดูแลผู้ใช้บริการได้อย่างรวดเร็ว

(6.2.3) **จัดให้ผู้ให้บริการออกบัตรต้องมีทางเลือกในการยืนยันตัวตนผู้ใช้บริการ**อย่างเหมาะสมตามระดับความเสี่ยงของธุรกรรม โดยต้องไม่จำกัดหรือไม่บังคับใช้วิธีการยืนยันตัวตนที่อาจทำให้ผู้ใช้บริการมีความเสี่ยงเพิ่มขึ้น เช่น ไม่กำหนดสัดส่วนบังคับให้ผู้ให้บริการออกบัตรต้องยืนยันตัวตนด้วยวิธีที่ผู้ใช้บริการไม่ต้องกรอก OTP สำหรับการทำธุรกรรมออนไลน์ (frictionless)

5.3.3 ด้านการรายงานและการเปิดเผยข้อมูล

(1) การรายงานข้อมูลต่อธนาคารแห่งประเทศไทย

ผู้ให้บริการออกบัตร ผู้ให้บริการรับบัตรและผู้ให้บริการระบบเครือข่ายบัตร ต้องดำเนินการ ดังนี้

(1.1) กรณีเกิดเหตุการณ์ภัยทุจริตจากการทำธุรกรรมด้วยบัตรที่สร้างความเสียหายต่อผู้ใช้บริการในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของผู้ให้บริการ ต้องรายงานเหตุการณ์ภัยทุจริตจากการทำธุรกรรมด้วยบัตรให้ธนาคารแห่งประเทศไทยทราบโดยเร็วตามช่องทางที่กำหนด

(1.2) ต้องจัดทำและจัดส่งแบบรายงานเพื่อประโยชน์ในการติดตามและประเมินประสิทธิผลของการบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตรและความเหมาะสมของนโยบายทางการ ตามรูปแบบ เงื่อนไขและแนวทางที่ธนาคารแห่งประเทศไทยกำหนด รวมถึงจัดทำและจัดส่งรายงานและข้อมูลอื่นเพิ่มเติมเป็นรายกรณีตามที่ธนาคารแห่งประเทศไทยร้องขอ

(2) การเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษ

กรณีที่ผู้ให้บริการออกบัตร ผู้ให้บริการรับบัตรและผู้ให้บริการระบบเครือข่ายบัตร ถูกเปรียบเทียบปรับหรือถูกกล่าวโทษอันเนื่องมาจากการปฏิบัติฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ของประกาศฉบับนี้ ต้องเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษดังกล่าว โดยให้ถือปฏิบัติตามประกาศและหลักเกณฑ์ของธนาคารแห่งประเทศไทยที่เกี่ยวข้องโดยอนุโลม เช่น ประกาศหลักเกณฑ์การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct)

ทั้งนี้ ธนาคารแห่งประเทศไทยขอสงวนสิทธิในการไม่ให้ผู้ให้บริการออกบัตร ผู้ให้บริการรับบัตรและผู้ให้บริการระบบเครือข่ายบัตร เปิดเผยข้อมูลการถูกดำเนินการทางกฎหมายตามที่ระบุข้างต้น หากเห็นว่าการเปิดเผยอาจกระทบต่อความปลอดภัยหรือความผาสุกของประชาชน รวมถึงประสิทธิผลของการบริหารจัดการภัยทุจริต

6. บทเฉพาะกาล

เมื่อประกาศฉบับนี้มีผลใช้บังคับแล้ว หากผู้ให้บริการใดไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในข้อ 5.3.1 ด้านธรรมาภิบาลและการกำหนดนโยบาย และข้อ 5.3.2 ด้านการบริหารจัดการภัยทุจริต ให้ผู้ให้บริการดำเนินการตามหลักเกณฑ์ดังกล่าวให้แล้วเสร็จภายใน 60 วันนับจากวันที่ประกาศฉบับนี้มีผลใช้บังคับ และเมื่อได้ปฏิบัติตามหลักเกณฑ์ที่กำหนดครบถ้วนแล้ว ให้แจ้งธนาคารแห่งประเทศไทย (ธปท.) ทราบโดยทันที เป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์

7. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ xx กันยายน 2568

(นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน
โทรศัพท์ 0 2283 5137, 0 2283 5058
ไปรษณีย์อิเล็กทรอนิกส์ psd-policyreg@bot.or.th

คำถาม – คำตอบแนบท้ายประกาศธนาคารแห่งประเทศไทย ที่ xx / 2568

เรื่อง การบริหารจัดการภัยทุจริตจากการทำธุรกรรมด้วยบัตร (Card Fraud Management)

ข้อ	คำถาม	คำตอบ
1	ขอบเขตการทำธุรกรรมด้วยบัตรที่ต้องปฏิบัติตามประกาศฉบับนี้ ครอบคลุมประเภทหรือลักษณะธุรกรรมใดบ้าง	หลักเกณฑ์ของประกาศฉบับนี้ครอบคลุมธุรกรรมทางการเงินที่มีการใช้บัตรเป็นสื่อในการทำธุรกรรม ทั้งบัตรเครดิต บัตรเดบิต บัตรเอทีเอ็ม หรือบัตรเงินอิเล็กทรอนิกส์ที่ใช้บริการผ่านระบบเครือข่ายบัตร เช่น การชำระค่าสินค้าและบริการแทนการใช้เงินสด การเบิกและถอนเงิน การโอนเงิน และการทำธุรกรรมอื่นใดที่เกี่ยวกับเงิน ผ่านช่องทางต่าง ๆ ที่ผู้ให้บริการกำหนดไว้ ทั้งในลักษณะที่มีการแสดงบัตร (card present) และการใช้ข้อมูลบัตรโดยไม่ต้องแสดงบัตร (card not present)
2	กรณีการให้บริการบัตรแก่ผู้ใช้บริการที่เป็นนิติบุคคล เข้าข่ายต้องปฏิบัติตามประกาศฉบับนี้ทุกข้อหรือไม่ และดำเนินการอย่างไร	ประกาศฉบับนี้ครอบคลุมถึงการให้บริการบัตรแก่ผู้ใช้บริการที่เป็นนิติบุคคลด้วย เช่น corporate card โดยต้องถือปฏิบัติตามหลักเกณฑ์ทุกข้อเช่นเดียวกับผู้ใช้บริการที่เป็นบุคคลธรรมดา สำหรับการปฏิบัติตามหลักเกณฑ์ในบางข้อ เช่น ข้อ 5.3.2 (3.1.2) การจัดให้มีระบบหรือช่องทางรองรับให้ผู้ใช้บริการสามารถบริหารจัดการความเสี่ยงด้วยตนเอง และข้อ 5.3.2 (3.1.4) การจัดให้มีการแจ้งเตือนผู้ใช้บริการโดยทันที เมื่อมีการทำธุรกรรม ให้ผู้ให้บริการดำเนินการกับนิติบุคคลหรือพนักงานที่ได้รับมอบหมายจากนิติบุคคลให้ควบคุมดูแลบัตรและการใช้งานบัตร
การป้องกันและจำกัดความเสียหาย		
3	ตัวอย่างธุรกรรมที่มีความเสี่ยงต่ำ มีธุรกรรมใดบ้าง	ธุรกรรมที่มีความเสี่ยงต่ำ เช่น ธุรกรรมชำระเงินมูลค่าต่ำกว่า 1,500 บาทหรือมูลค่าที่ผู้ให้บริการที่เกี่ยวข้อง ทั้งผู้ให้บริการออกบัตร ผู้ให้บริการรับบัตร และผู้ให้บริการระบบเครือข่ายบัตร กำหนดร่วมกันเป็นมาตรฐานอุตสาหกรรม และธุรกรรมการชำระเงินอัตโนมัติ (recurring payment) ที่

ข้อ	คำถาม	คำตอบ
		ผู้ใช้บริการได้ตกลงยินยอมไว้กับผู้ให้บริการอย่างชัดเจนแล้ว ทั้งนี้ ในกรณีที่ผู้ใช้บริการเกิดปัญหาหรือเหตุภัยทุจริตจากการทำธุรกรรมที่มีความเสี่ยงต่ำข้างต้น ผู้ให้บริการยังคงมีหน้าที่และความรับผิดชอบในการดูแลผู้ใช้บริการอย่างรวดเร็ว โปร่งใส และเป็นธรรม โดยปฏิบัติให้เป็นไปตามหลักเกณฑ์ในข้อ (4) การแก้ไขสถานการณ์และการดูแลผู้ใช้บริการ (response)
การจัดการบัตรที่มีความเสี่ยงที่อาจถูกใช้ในการกระทำความผิด และบัตรที่มีรายชื่อผู้ใช้บริการเป็นเจ้าของบัญชีม้า		
4	การจำกัดความเสียหายและจัดการบัตรที่มีรายชื่อผู้ใช้บริการเป็นเจ้าของบัญชีม้า ให้ดำเนินการอย่างไร	กรณีบัตรเดบิตและบัตรเอทีเอ็ม ซึ่งเป็นสื่อการทำธุรกรรมทางการเงินที่เชื่อมโยงกับบัญชีเงินฝาก ให้ดำเนินการตามหลักเกณฑ์ของประกาศธนาคารแห่งประเทศ ที่ 19/2568 เรื่อง มาตรฐานและมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีสำหรับสถาบันการเงิน ลงวันที่ 25 กรกฎาคม 2568 ในข้อ 4.2.4 (2) - (4) เป็นขั้นต่ำ กรณีบัตรเครดิต ให้ดำเนินการตามหลักเกณฑ์ของประกาศธนาคารแห่งประเทศไทย ที่ xx/2568 เรื่อง มาตรฐานและมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยี สำหรับผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงิน ลงวันที่ xxx ในข้อ 4.2.4 การจำกัดความเสียหายและจัดการบัญชีม้า (2) - (4) เป็นขั้นต่ำ กรณีบัตรเงินอิเล็กทรอนิกส์ที่ใช้บริการผ่านระบบเครือข่ายบัตร ซึ่งเป็นสื่อการทำธุรกรรมทางการเงินที่เชื่อมโยงกับบัญชีเงินอิเล็กทรอนิกส์ ให้ดำเนินการตามหลักเกณฑ์ของประกาศธนาคารแห่งประเทศไทย ที่ xx/2568 เรื่อง มาตรฐานและมาตรการเพื่อป้องกันอาชญากรรม

ข้อ	คำถาม	คำตอบ
		ทางเทคโนโลยี สำหรับผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงิน ลงวันที่ xxx ในข้อ 4.2.4 การจำกัดความเสียหายและจัดการบัญชีม้า (2) - (4) เป็นขั้นต่ำ
การรายงานเหตุการณ์ภัยทุจริตและการสื่อสารต่อสาธารณชน		
5	ความเสียหายต่อผู้ใช้บริการในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของผู้ให้บริการพิจารณาอย่างไร	การพิจารณาให้พิจารณาจากผลกระทบดังนี้ (1) ผลกระทบต่อผู้ใช้บริการจำนวนมาก (2) ผลกระทบต่อระบบการเงินและการชำระเงิน เช่น กระทบต่อผู้ให้บริการรายหลาย กระทบต่อระบบงานกลางที่มีนัยสำคัญ (3) ผลกระทบต่อชื่อเสียงของผู้ให้บริการ เช่น มูลค่าความเสียหายจำนวนสูง
ความร่วมมือ		
6	การเปิดเผยหรือแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับเหตุการณ์ภัยทุจริตผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามที่กำหนดไว้ในกฎหมายว่าด้วยมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี หมายถึงระบบใด	ผู้ให้บริการออกบัตรและผู้ให้บริการรับบัตรต้องมีกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลภัยทุจริตร่วมกับผู้ให้บริการทางการเงินอื่น ๆ โดยอย่างน้อยต้องเชื่อมต่อและแลกเปลี่ยนข้อมูลระหว่างกันผ่านระบบ Central Fraud Registry (CFR)
การรายงานข้อมูลต่อธนาคารแห่งประเทศไทย		
7	การรายงานเหตุการณ์ภัยทุจริตจากการทำธุรกรรมด้วยบัตรให้ธนาคารแห่งประเทศไทย (ธปท.) ทราบโดยเร็วตามช่องทางที่กำหนด หมายถึงช่องทางใด	ผู้ให้บริการต้องแจ้งผู้ประสานงาน ธปท. (เจ้าหน้าที่สัมพันธ์ (relationship manager)) ทันที ผ่านระบบ event report ทั้งนี้ ผู้ให้บริการยังคงต้องจัดทำและจัดส่งรายงานให้เป็นไปตามหลักเกณฑ์อื่น ๆ ที่กำหนดไว้ด้วย