ธนาคารแห่งประเทศไทย

29 มีนาคม 2566

เรียน ผู้จัดการ

สถาบันการเงินทุกแห่ง

สถาบันการเงินเฉพาะกิจทุกแห่ง

ผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ที่มิใช่สถาบันการเงิน

ที่ ธปท.ฝนช.(02) ว.224/2566 เรื่อง นำส่งแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน

ด้วยปัจจุบันภัยทุจริตจากการทำธุรกรรมทางการเงินมีแนวโน้มเพิ่มขึ้นและมีรูปแบบใหม่ สร้างความเสียหายต่อประชาชนในวงกว้าง และส่งผลกระทบต่อความน่าเชื่อถือของระบบการชำระเงินโดยรวม ขณะที่ผู้ให้บริการทางการเงินมีการบริหารจัดการภัยทุจริตที่แตกต่างกันในทางปฏิบัติและยังมีส่วนที่ต้องปรับปรุงและยกระดับเพื่อให้รับมือกับภัยทุจริตรูปแบบใหม่ได้เท่าทัน

ธนาคารแห่งประเทศไทย (ธปท.) เห็นควรให้ผู้ให้บริการทางการเงินทั้งสถาบันการเงิน สถาบันการเงินเฉพาะกิจ และผู้ให้บริการชำระเงินภายใต้การกำกับทุกราย ยกระดับการบริหารจัดการภัยทุจริตให้เป็นความเสี่ยงสำคัญขององค์กร รวมถึงจัดการเหตุการณ์และดูแลคุ้มครองผู้ใช้บริการได้อย่างเพียงพอเหมาะสม ธปท. จึงได้ออกแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงินให้ผู้ให้บริการทางการเงินใช้เป็นแนวทางขั้นต่ำในการถือปฏิบัติ โดยเริ่มต้นใช้ตั้งแต่วันที่ 29 มีนาคม 2566 สรุปสาระสำคัญที่ขอให้ผู้ให้บริการทางการเงินดำเนินการ ดังนี้

1. **ด้านธรรมาภิบาล** กำหนดนโยบาย แนวปฏิบัติและกระบวนการที่เกี่ยวข้องกับการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน รวมถึงกำกับดูแลให้มีการปฏิบัติตามนโยบายและแนวปฏิบัติที่วางไว้อย่างเคร่งครัด

2. **ด้านการบริหารจัดการภัยทุจริต** จัดให้มีการประเมินการปฏิบัติตามแนวนโยบายฉบับนี้ รวมทั้งวางแผนดำเนินการเพื่อปิด gap ที่ชัดเจน และขอให้ผู้ที่ทำหน้าที่กำกับการปฏิบัติตามหลักเกณฑ์มีส่วนร่วมในการประเมินและติดตามแผนการดำเนินการดังกล่าว

3. การรายงานเหตุการณ์ทุจริตให้ ธปท. ทราบตามแนวนโยบายฉบับนี้ ให้ผู้ให้บริการทางการเงินแจ้งผ่านระบบ Event Report

ทั้งนี้ ท่านสามารถดาวน์โหลดแนวนโยบายดังกล่าวได้ทางเว็บไซต์ของ ธปท. ที่ https://www.bot.or.th/App/FIPCS/Thai/PFIPCS_list.aspx

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ)
ผู้ว่าการ

สิ่งที่ส่งมาด้วย แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน

ฝ่ายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน และ
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6574, 0 2356 7695

หมายเหตุ [X] ธนาคารได้จัดประชุมชี้แจงในวันที่ 20 ตุลาคม 2565 และ 2 กุมภาพันธ์ 2566
[ ] ไม่มีการประชุมชี้แจง

แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน

29 มีนาคม 2566

ธนาคารแห่งประเทศไทย

จัดทำโดย

ฝ่ายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สายกำกับระบบการชำระเงินและคุ้มครองผู้ใช้บริการทางการเงิน

ธนาคารแห่งประเทศไทย

โทรศัพท์ 0 2283 6574, 0 2356 7695

email: TSD-techpolicy@bot.or.th, PSDpolicy@bot.or.th

ฝนชว90-กส65002-25660329

กส650	วันที่ 29 มี.ค. 2566

สารบัญ

หัวข้อ **หน้า**

แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน

---

1. หลักการและเหตุผล

ปัจจุบันการทำธุรกรรมทางการเงินสามารถทำผ่านช่องทางการให้บริการทางการเงินได้หลากหลาย เช่น สาขาอิเล็กทรอนิกส์ ช่องทางดิจิทัล เพื่ออำนวยความสะดวกต่อผู้ใช้บริการให้เข้าถึงบริการทางการเงินและการชำระค่าสินค้าบริการได้หลากหลายรูปแบบ สะดวก รวดเร็ว และครอบคลุมพื้นที่การให้บริการมากขึ้น ดังนั้น การบริหารจัดการความเสี่ยงอย่างรัดกุมเพียงพอจึงเป็นเรื่องสำคัญ เพื่อป้องกันช่องโหว่ในการทำทุจริตจากการทำธุรกรรมทางการเงินที่อาจก่อให้เกิดความเสียหายต่อผู้ใช้บริการได้ ผู้ให้บริการทางการเงินจึงควรให้ความสำคัญในการสร้างสมดุลระหว่างการอำนวยความสะดวกในการทำธุรกรรมที่ง่ายขึ้นของผู้ใช้บริการ การติดตามและบริหารจัดการความเสี่ยงที่รัดกุมและเท่าทันเพียงพอกับสภาพแวดล้อมทางการเงินที่เปลี่ยนแปลงไป และการคุ้มครองผู้ใช้บริการอย่างเหมาะสมเป็นธรรม

การบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงินเป็นเรื่องที่ผู้ให้บริการทางการเงินต้องตระหนักและให้ความสำคัญมากขึ้น เพื่อลดโอกาสที่ผู้ใช้บริการอาจตกเป็นเหยื่อของมิจฉาชีพจากภัยทุจริตต่าง ๆ ที่มีการพัฒนาเปลี่ยนแปลงรูปแบบอย่างรวดเร็ว เช่น การสวมรอยหรือขโมยข้อมูลไปใช้ทำธุรกรรมทางการเงิน การหลอกลวงให้โอนเงิน การถูกบังคับหรือหลอกลวงให้เปิดบัญชี เป็นต้น รวมทั้งดูแลให้ลูกค้าได้รับการแจ้งเตือนอย่างทันกาล เพื่อจำกัดความเสียหายไม่ให้ขยายตัว หรือลุกลามเป็นวงกว้าง และการดูแลให้ได้รับการช่วยเหลือเยียวยาในเวลาที่เหมาะสมอย่างรวดเร็ว

ธนาคารแห่งประเทศไทยจึงได้กำหนด**แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน** โดยมีหลักการเพื่อให้เป็นมาตรฐานสำหรับการให้บริการทางการเงิน ทั้งด้านธรรมาภิบาลและด้านบริหารจัดการภัยทุจริตเพื่อให้มีมาตรการป้องกัน ตรวจจับภัยทุจริต ตอบสนองและรับมือต่อเหตุการณ์ที่เกิดขึ้น รวมทั้งสร้างความร่วมมือระหว่างผู้ให้บริการทางการเงินและหน่วยงานที่เกี่ยวข้อง เพื่อสร้างความน่าเชื่อถือต่อระบบการเงิน และระบบการชำระเงิน

2. ขอบเขตการใช้

แนวนโยบายฉบับนี้ให้สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน รวมถึงผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน นำไปปฏิบัติ

3. เนื้อหา

3.1 นิยาม

ภายใต้แนวนโยบายฉบับนี้

“ผู้ให้บริการทางการเงิน” หมายความว่า สถาบันการเงิน และสถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับและผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน

“การทำธุรกรรมทางการเงิน” หมายความว่า การทำธุรกรรมทางการเงินที่ผู้ให้บริการทางการเงินให้บริการ เช่น การเปิดบัญชี การสมัครใช้บริการ การฝากเงิน การถอนเงิน การโอนเงิน และการชำระค่าสินค้าและบริการ โดยผ่านช่องทางการให้บริการครอบคลุม สาขาทั่วไป สาขาอิเล็กทรอนิกส์ ช่องทางดิจิทัล (digital channels) หรือช่องทางให้บริการอื่นที่ธนาคารแห่งประเทศไทยอนุญาตเพิ่มเติมทั้งที่เป็นการทำธุรกรรมทางการเงินผ่านบัตร บริการเงินอิเล็กทรอนิกส์ หรือผ่านสื่ออื่น เช่น QR code

“สาขาทั่วไป” หมายความว่า ช่องทางให้บริการที่มีสถานที่ทำการที่แน่นอนและให้บริการโดยพนักงานของผู้ให้บริการทางการเงิน ซึ่งอาจมีการให้บริการโดยเครื่องอิเล็กทรอนิกส์บริเวณภายในหรือหน้าช่องทางให้บริการดังกล่าวด้วยก็ได้

“สาขาอิเล็กทรอนิกส์” หมายความว่า ช่องทางให้บริการที่มีสถานที่ตั้งหรือสถานที่ทำการที่แน่นอนด้วยเครื่องอิเล็กทรอนิกส์ โดยผู้ใช้บริการดำเนินการด้วยตนเอง ซึ่งผู้ให้บริการทางการเงินอาจจัดให้มีพนักงานคอยให้คำแนะนำหรือช่วยเหลือผู้ใช้บริการในการใช้เครื่องอิเล็กทรอนิกส์ดังกล่าว เช่น เครื่องถอนเงินสดอัตโนมัติ (Automatic Teller Machine: ATM) หรือเครื่องฝากเงินสดอัตโนมัติ (Cash Deposit Machine: CDM) ทั้งนี้ ไม่รวมถึงเครื่องอิเล็กทรอนิกส์ที่ให้บริการบริเวณภายในหรือหน้าสาขาทั่วไป

“ช่องทางดิจิทัล” หมายความว่า ช่องทางให้บริการที่เป็นการให้บริการทางอินเทอร์เน็ต (internet banking) อุปกรณ์เคลื่อนที่ (mobile banking) และช่องทางดิจิทัลอื่น ๆ ที่ธนาคารแห่งประเทศไทยอนุญาตเพิ่มเติม

“บัตร” หมายความว่า บัตรเดบิต หรือบัตรเครดิต

“บัตรเดบิต” หมายความว่า บัตรอิเล็กทรอนิกส์ที่ผู้ให้บริการทางการเงินออกให้แก่ผู้ใช้บริการเพื่อใช้ชำระค่าสินค้า ค่าบริการ หรือค่าอื่นใด แทนการชำระด้วยเงินสด หรือเพื่อใช้เบิก ถอน โอน หรือทำธุรกรรมอื่นใดที่เกี่ยวกับเงิน ตามมูลค่าของเงินที่ผู้ใช้บริการได้ฝากไว้กับผู้ให้บริการทางการเงิน

“บัตรเครดิต” หมายความว่า บัตรอิเล็กทรอนิกส์ที่ผู้ให้บริการทางการเงินออกให้แก่ผู้ใช้บริการเพื่อใช้ชำระค่าสินค้า ค่าบริการ หรือค่าอื่นใด แทนการชำระด้วยเงินสด หรือเพื่อใช้เบิก ถอน โอน หรือทำธุรกรรมอื่นใดที่เกี่ยวกับเงิน และผู้ให้บริการทางการเงินจะเรียกให้ผู้ใช้บริการชำระเงินในภายหลัง

“ผู้ให้บริการทางการเงินที่เกี่ยวข้องกับการทำธุรกรรมการชำระเงินผ่านบัตร” หมายความว่า ผู้ประกอบธุรกิจที่ได้รับอนุญาตให้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน ซึ่งมีลักษณะหรือประเภทการให้บริการ ดังต่อไปนี้

(1) การให้บริการบัตรเครดิต หรือบัตรเดบิต

(2) การให้บริการแก่ผู้รับบัตร

(3) การให้บริการสนับสนุนบริการแก่ผู้รับบัตร

“ผู้ให้บริการระบบเครือข่ายบัตร” หมายความว่า ผู้ประกอบธุรกิจที่ได้รับอนุญาตหรือขึ้นทะเบียนให้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน ซึ่งมีการให้บริการระบบเครือข่ายบัตร

“คณะกรรมการ” หมายความว่า คณะกรรมการบริษัทหรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย

“ธปท.” หมายความว่า ธนาคารแห่งประเทศไทย

3.2 แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน

แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน มีวัตถุประสงค์ให้ผู้ให้บริการทางการเงินยกระดับการดูแลและจัดการเหตุการณ์ทุจริตได้อย่างเพียงพอและทันท่วงที เพื่อลดความเสี่ยง ความเสียหาย และผลกระทบต่อทั้งผู้ใช้บริการและผู้ให้บริการทางการเงิน รวมถึงความเชื่อมั่นต่อเสถียรภาพของระบบการเงินและระบบการชำระเงิน โดยผู้ให้บริการทางการเงินต้องดำเนินการดังนี้

3.2.1 ผู้ให้บริการทางการเงินทุกแห่งต้องถือปฏิบัติตามแนวนโยบายฉบับนี้เป็นมาตรฐานขั้นต่ำเพื่อให้มีนโยบาย มาตรการ และการติดตามดูแลการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงินทั้งด้านธรรมาภิบาลและด้านบริหารจัดการภัยทุจริต

สำหรับการให้บริการที่เกี่ยวข้องกับการทำธุรกรรมการชำระเงินผ่านบัตร ให้ปฏิบัติเพิ่มเติมตามข้อกำหนดในเอกสารแนบ 1 และการให้บริการที่เกี่ยวข้องกับบัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์เฉพาะที่ให้บริการโอนเงินไปยังบัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์ที่ให้บริการโดยผู้ให้บริการทางการเงินอื่นได้ สำหรับผู้ใช้บริการรายย่อย ให้ปฏิบัติเพิ่มเติมตามข้อกำหนดในเอกสารแนบ 2 ด้วย

3.2.2 ผู้ให้บริการทางการเงินต้องจัดให้มีนโยบายและมาตรการเกี่ยวกับการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ดังต่อไปนี้

(1) ด้านธรรมาภิบาล

คณะกรรมการและผู้บริหารระดับสูงของผู้ให้บริการทางการเงินควรตระหนักถึงบทบาทหน้าที่ในการกำกับดูแลให้ผู้ให้บริการทางการเงินมีการบริหารจัดการเหตุการณ์ทุจริตอย่างเท่าทันและเหมาะสมกับลักษณะความซับซ้อนของภัยทุจริตที่เกิดขึ้น ตลอดจนให้ความสำคัญกับการป้องกันและรับมือภัยทุจริตโดยกำหนดให้เป็นความเสี่ยงสำคัญที่องค์กรต้องมีการบริหารจัดการร่วมกันอย่างเป็นบูรณาการ โดยผู้ให้บริการทางการเงินต้องจัดให้มีแนวปฏิบัติ ดังนี้

(1.1) กำหนดให้มีคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทำหน้าที่กำหนดนโยบายและกำกับดูแลอย่างชัดเจนเพื่อให้องค์กรมีแนวทางบริหารจัดการภัยทุจริตอย่างครอบคลุมบูรณาการทั้งในเชิงป้องกัน ตรวจจับ ตอบสนองและรับมือกับเหตุการณ์ภัยทุจริต ติดตามเหตุการณ์ภัยทุจริตที่เกิดขึ้น และดำเนินการลดความเสี่ยงและผลกระทบอย่างทันกาล รวมทั้งประเมินความพร้อมและประสิทธิภาพของการจัดการภัยทุจริตขององค์กร ทั้งในด้านบุคลากร กระบวนการ เทคโนโลยีและเครื่องมือที่ใช้ในการจัดการภัยทุจริตอย่างสม่ำเสมอ เพื่อผลักดันให้มีการพัฒนาที่เท่าทันกับภัยทุจริตอย่างต่อเนื่อง

ทั้งนี้ กรณีเกิดเหตุการณ์ทุจริตจากการทำธุรกรรมทางการเงินที่ก่อให้เกิดความเสียหายกับผู้ใช้บริการในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของผู้ให้บริการทางการเงิน ผู้ให้บริการทางการเงินต้องรายงานให้คณะกรรมการหรือผู้บริหารระดับสูงที่รับผิดชอบรับทราบโดยเร็ว เพื่อสั่งการให้มีการดำเนินการลดผลกระทบและจำกัดความเสียหายที่เกิดขึ้น

(1.2) จัดให้มีนโยบายในการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงินที่ชัดเจนเป็นลายลักษณ์อักษร ได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย รวมทั้งจัดให้มีการทบทวนและปรับปรุงนโยบาย อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์หรือการ

เปลี่ยนแปลงที่ส่งผลกระทบอย่างมีนัยสำคัญกับนโยบายและมาตรการที่กำหนด โดยนโยบายดังกล่าว ต้องครอบคลุมอย่างน้อย

(1.2.1) บทบาทหน้าที่ของคณะกรรมการที่กำกับดูแลและหน่วยงานที่รับผิดชอบ

(1.2.2) แนวทาง กระบวนการจัดการ การรายงานเหตุการณ์ภัยทุจริต และการสื่อสารที่เหมาะสมกับความเสี่ยงและผลกระทบที่เกิดขึ้น

(1.2.3) ติดตามและวัดประสิทธิภาพของการจัดการภัยทุจริตอย่างต่อเนื่อง

ทั้งนี้ ผู้ให้บริการทางการเงินต้องจัดให้มีการสื่อสารเผยแพร่นโยบายและแนวปฏิบัติเพื่อให้ทุกฝ่ายงานในองค์กรนำไปปฏิบัติได้อย่างเหมาะสม

(1.3) จัดให้มีการประเมิน วัดผล และติดตามประสิทธิภาพและประสิทธิผลของการจัดการภัยทุจริต โดยรายงานผลประเมินดังกล่าวต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายอย่างต่อเนื่อง นอกจากนี้ ผู้ให้บริการทางการเงินต้องมีการกำหนดเป้าหมายและตัวชี้วัดประสิทธิภาพที่ครอบคลุมและชัดเจนเหมาะสมทั้งในเชิงป้องกัน ตรวจจับ ตอบสนองและรับมือกับเหตุการณ์ภัยทุจริตและการดูแลลูกค้าที่ได้รับผลกระทบอย่างเพียงพอเหมาะสม

ทั้งนี้ หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง หน่วยงานที่ทำหน้าที่กำกับการปฏิบัติตามกฎเกณฑ์ และหน่วยงานที่ทำหน้าที่ตรวจสอบภายใน ควรมีส่วนร่วมในการผลักดันให้องค์กรมีการบริหารจัดการภัยทุจริตอย่างเท่าทัน โดยกำหนดกรอบแนวทางบริหารความเสี่ยงองค์กรและกรอบแนวทางการตรวจสอบให้ครอบคลุมความเสี่ยงด้านการทุจริต เพื่อให้ผู้ให้บริการทางการเงินมีมาตรการจัดการความเสี่ยงที่เหมาะสมทันกาล

(1.4) สร้างความตระหนักรู้เกี่ยวกับการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงินอย่างบูรณาการทั่วทั้งองค์กร ครอบคลุมคณะกรรมการ ผู้บริหารระดับสูงและบุคลากรของผู้ให้บริการทางการเงิน เพื่อให้มีความรู้ความเข้าใจที่เพียงพอต่อการกำกับดูแลและการบริหารจัดการภัยทุจริตอย่างเท่าทันกับภัยรูปแบบใหม่ ๆ ที่อาจเกิดขึ้น นอกจากนี้ ผู้ให้บริการทางการเงิน ต้องมีการสร้างความตระหนักรู้เตือนภัยแก่ผู้ใช้บริการไม่ให้ตกเป็นเหยื่อของมิจฉาชีพอย่างต่อเนื่องและทันกาล เพื่อให้ผู้ใช้บริการมีความระมัดระวังในการทำธุรกรรมทางการเงินมากขึ้น เช่น แจ้งเตือนภัยทุจริตและพฤติกรรมการหลอกลวงใหม่ ๆ สื่อสารให้ทราบถึงความเสี่ยงและความผิดจากการรับจ้างเปิดบัญชี วิธีการทำธุรกรรมทางการเงินอย่างปลอดภัย เป็นต้น

(2) ด้านบริหารจัดการภัยทุจริต

ผู้ให้บริการทางการเงินต้องจัดให้มีกรอบการดำเนินการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงินที่ชัดเจน อย่างน้อยครอบคลุมการป้องกันภัย (Protection) การตรวจจับ (Detection) การตอบสนองและรับมือ (Response) และด้านความร่วมมือ (Collaboration) ดังนี้

(2.1) การป้องกันภัย (Protection)

ผู้ให้บริการทางการเงินต้องกำหนดมาตรการป้องกันภัยทุจริตจากการทำธุรกรรมทางการเงินครอบคลุมตั้งแต่ต้นจนจบกระบวนการ (end-to-end process) และสอดคล้องตาม

มาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป เพื่อให้เท่าทันและเหมาะสมกับปริมาณ รูปแบบ และสภาพแวดล้อมทางการเงินที่เปลี่ยนแปลงไป โดยมีแนวปฏิบัติดังนี้

(2.1.1) จัดให้มีการนำเหตุการณ์และปัจจัยความเสี่ยงที่อาจเกิดภัยทุจริตจากการทำธุรกรรมทางการเงินมาใช้ในการพิจารณาตั้งแต่เริ่มต้นการออกแบบ พัฒนา หรือปรับปรุงผลิตภัณฑ์ทางการเงิน เพื่อให้การให้บริการมีระบบและมาตรการป้องกันภัยทุจริตที่อาจเกิดขึ้น เช่น การสวมรอยสมัครใช้บริการทางการเงินแทนผู้ใช้บริการตัวจริง การถูกผู้ไม่ประสงค์ดีหลอกลวงเพื่อให้เหยื่อเปิดเผยข้อมูลส่วนบุคคลหรือให้ทำธุรกรรมทางการเงิน การถูกผู้ไม่ประสงค์ดีทำธุรกรรมทางการเงินโดยไม่ได้รับอนุญาตแทนผู้ใช้บริการตัวจริง เป็นต้น

(2.1.2) จัดให้มีมาตรการการป้องกันภัยทุจริตจากการทำธุรกรรมทางการเงินทั้งภายในและภายนอกองค์กร ตั้งแต่การสมัครหรือเปิดใช้บริการ การทำธุรกรรม จนถึงการปิดหรือยกเลิกการใช้บริการ โดยมาตรการดังกล่าวให้ครอบคลุมอย่างน้อย

- มีกระบวนการและระบบการพิสูจน์และยืนยันตัวตนในการทำธุรกรรมตามระดับความเสี่ยงของผลิตภัณฑ์และช่องทางการให้บริการ โดยให้เป็นไปตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง เช่น หลักเกณฑ์ของกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การรู้จักตัวตนลูกค้าสำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน หลักเกณฑ์การรู้จักลูกค้าสำหรับการเปิดใช้บริการเงินอิเล็กทรอนิกส์ เป็นต้น
- มีกระบวนการและระบบในการรักษาความปลอดภัยของข้อมูลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และสอดคล้องกับหลักเกณฑ์ที่เกี่ยวข้องตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป เช่น ISO/IEC 27001 เป็นต้น
- มีระบบหรือช่องทางรองรับให้ผู้ใช้บริการสามารถกำหนด การตั้งค่าการทำธุรกรรม และจัดให้มีการแจ้งเตือนการทำธุรกรรมผ่านช่องทางต่าง ๆ เช่น ข้อความสั้น (SMS) อีเมล โซเชียลมีเดีย เพื่อให้ผู้ใช้บริการสามารถบริหารจัดการความเสี่ยงในการทำธุรกรรมได้สอดคล้องกับความต้องการของตนเอง และรับทราบการทำธุรกรรมต่าง ๆ อย่างเหมาะสมทันกาล

(2.1.3) ทบทวนและปรับปรุงทั้งกระบวนการและระบบป้องกันภัยทุจริตจากการทำธุรกรรมทางการเงินอย่างสม่ำเสมอ รวมทั้งนำเทคโนโลยีหรือวิธีการใหม่ ๆ เช่น การยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) มาใช้เพื่อยกระดับการป้องกันให้เท่าทันและสอดคล้องกับสภาพแวดล้อมทางการเงินที่เปลี่ยนแปลงไป

(2.2) การตรวจจับ (Detection)

ผู้ให้บริการทางการเงินต้องมีมาตรการในการตรวจจับและติดตามความผิดปกติจากการทำธุรกรรมทางการเงินอย่างมีประสิทธิภาพและเป็นลักษณะเชิงรุก เพื่อให้สามารถตรวจพบความเสี่ยงและภัยทุจริต เฝ้าระวังหรือระงับธุรกรรมต้องสงสัย และแจ้งเตือนผู้ใช้บริการหรือผู้ที่เกี่ยวข้องได้อย่างรวดเร็วทันกาล รวมทั้งสามารถจำกัดความเสียหายไม่ให้ขยายตัวหรือลุกลามเป็นวงกว้าง โดยมีแนวปฏิบัติดังนี้

(2.2.1) จัดให้มีบุคลากร กระบวนการ และระบบในการตรวจจับและติดตามความผิดปกติจากการทำธุรกรรมทางการเงินอย่างเพียงพอเหมาะสม เพื่อให้สามารถเฝ้าระวังและจำกัดความเสียหายจากภัยทุจริตได้อย่างทันท่วงที

(2.2.2) กำหนดเงื่อนไขในการตรวจจับให้ครอบคลุมรูปแบบภัยทุจริตในแต่ละช่องทางของการให้บริการทางการเงินสอดคล้องกับระดับความเสี่ยงของภัยทุจริตและผู้ใช้บริการ เช่น ธุรกรรมที่มีความถี่สูง ธุรกรรมชำระเงินผ่านบัตรจากร้านค้าที่มีความเสี่ยง ธุรกรรมที่โอนเงินไปยังผู้ต้องสงสัย ธุรกรรมที่ปกติไม่มีการเคลื่อนไหวแต่เกิดการทำธุรกรรมผิดปกติ เป็นต้น โดยให้สามารถแจ้งเตือนได้อย่างทันกาล มีกระบวนการในการทบทวนและปรับปรุงเงื่อนไขและประสิทธิภาพในการตรวจจับอย่างสม่ำเสมอและเป็นลักษณะเชิงรุก (proactive detection) เพื่อให้เท่าทันกับสถานการณ์และรูปแบบการทุจริตใหม่ ๆ และสามารถระงับเหตุการณ์ทุจริตและป้องกันความเสียหายที่อาจเกิดขึ้นเป็นวงกว้างได้อย่างเท่าทัน

(2.2.3) กำหนดกระบวนการและช่องทางในการรับแจ้งเหตุการณ์ต้องสงสัยหรือเหตุการณ์ทุจริตจากการทำธุรกรรมทางการเงินทั้งจากภายในและภายนอกองค์กร เช่น ช่องทางติดต่อทางโทรศัพท์ ช่องทางอิเล็กทรอนิกส์ ที่ผู้ใช้บริการสามารถติดต่อได้เพื่อให้การติดตามตรวจสอบเหตุการณ์ทุจริตที่อาจเกิดขึ้นเป็นไปอย่างทันกาล

(2.2.4) ทบทวนและปรับปรุงทั้งกระบวนการและระบบตรวจจับภัยทุจริตจากการทำธุรกรรมทางการเงินอย่างสม่ำเสมอ รวมทั้งอาจพิจารณานำเทคโนโลยีใหม่ ๆ เช่น ระบบวิเคราะห์ข้อมูล (data analytics) เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence) มาใช้เพิ่มประสิทธิภาพในการตรวจจับภัยทุจริต ให้เท่าทันและสอดคล้องกับสภาพแวดล้อมทางการเงินที่เปลี่ยนแปลงไป

(2.3) การตอบสนองและรับมือ (Response)

ผู้ให้บริการทางการเงินต้องมีมาตรการตอบสนองและรับมือต่อเหตุการณ์ภัยทุจริตจากการทำธุรกรรมทางการเงิน เพื่อช่วยเหลือและเยียวยาผู้ใช้บริการที่ได้รับผลกระทบได้อย่างเหมาะสมทันเหตุการณ์และเป็นธรรม โดยมีแนวปฏิบัติดังนี้

(2.3.1) กำหนดกระบวนการตอบสนองและรับมือต่อเหตุการณ์ภัยทุจริตจากการทำธุรกรรมทางการเงินอย่างครอบคลุม ชัดเจน และสอดคล้องตามระดับความเสี่ยงของภัยทุจริต โดยกระบวนการดังกล่าวควรครอบคลุม การแก้ไขสถานการณ์ การจำกัดความเสียหาย การช่วยเหลือและเยียวยาผู้ใช้บริการที่ได้รับผลกระทบ การสื่อสารและประชาสัมพันธ์ต่อสาธารณะ พร้อมทั้งจัดให้มีการซักซ้อมเพื่อให้ฝ่ายงานที่เกี่ยวข้องเข้าใจบทบาทหน้าที่ แนวทางและกระบวนการในการตอบสนองและรับมือต่อเหตุการณ์ทุจริตในรูปแบบต่าง ๆ

(2.3.2) กำหนดข้อตกลงในการใช้บริการ (Service Level Agreement) ในการดูแลผู้ใช้บริการที่ได้รับผลกระทบจากความเสียหายที่เกิดขึ้นจากเหตุการณ์ทุจริตให้ชัดเจน เช่น การแจ้งให้ผู้ใช้บริการทราบเมื่อเกิดเหตุการณ์ การติดต่อกลับผู้ใช้บริการอย่างรวดเร็วภายในเวลาที่เหมาะสมหลังได้รับแจ้งเหตุการณ์เข้าข่ายทุจริตจากผู้ใช้บริการ การเยียวยาให้ผู้ใช้บริการเมื่อพิสูจน์ได้ว่าผู้ใช้บริการได้รับความเสียหาย เป็นต้น

(2.3.3) กำหนดกระบวนการในการรายงานเหตุการณ์ทุจริตจากการทำธุรกรรมทางการเงินแก่คณะกรรมการหรือผู้บริหารระดับสูงที่มีหน้าที่รับผิดชอบเหมาะสมตามระดับความรุนแรงของเหตุการณ์ ทั้งนี้ กรณีที่เกิดความเสียหายกับผู้ใช้บริการในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของผู้ให้บริการทางการเงิน ต้องรายงานเหตุการณ์ทุจริตให้ ธปท. ทราบโดยเร็วตามช่องทางที่กำหนด โดยผู้ให้บริการทางการเงินสามารถแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

(2.3.4) กรณีเกิดเหตุการณ์ทุจริตจากการทำธุรกรรมทางการเงินที่ก่อให้เกิดความเสียหายกับผู้ใช้บริการในวงกว้าง ผู้ให้บริการทางการเงินต้องยกระดับการช่วยเหลือและเยียวยา รวมถึงสื่อสารและประชาสัมพันธ์เพื่อชี้แจงและทำความเข้าใจกับผู้ใช้บริการเกี่ยวกับปัญหาและผลกระทบที่เกิดขึ้นอย่างทันกาล เพื่อไม่ให้ผู้ใช้บริการเกิดความเข้าใจที่คลาดเคลื่อนหรือตื่นตระหนกจนเกินไป

(2.4) ความร่วมมือ (Collaboration)

ผู้ให้บริการทางการเงินควรสร้างกลไกความร่วมมือและแลกเปลี่ยนข้อมูลเกี่ยวกับการป้องกัน การตรวจจับ การตอบสนองและรับมือภัยทุจริตระหว่างผู้ให้บริการทางการเงินและหน่วยงานภายนอกที่เกี่ยวข้อง เพื่อยกระดับการจัดการภัยทุจริตจากการทำธุรกรรมทางการเงินให้มีประสิทธิภาพยิ่งขึ้น โดยมีแนวปฏิบัติดังนี้

(2.4.1) สร้างกลไกความร่วมมือและแลกเปลี่ยนข้อมูล โดยกำหนดแนวทาง กระบวนการ และช่องทางการสื่อสารประสานงานในการป้องกัน ตรวจจับ ตอบสนองและรับมือภัยทุจริตจากการทำธุรกรรมทางการเงินระหว่างผู้ให้บริการทางการเงินกับหน่วยงานกำกับดูแลหรือหน่วยงานที่เกี่ยวข้อง เช่น สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานตำรวจแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ ผู้ประกอบกิจการโทรคมนาคม เป็นต้น รวมทั้งควรมอบหมายฝ่ายงานที่ทำหน้าที่ดูแลและประสานงานร่วมกับหน่วยงานอื่นอย่างชัดเจน

ทั้งนี้ การแลกเปลี่ยนข้อมูล อาจพิจารณาจัดให้มีระบบการแลกเปลี่ยนข้อมูลที่เกี่ยวกับการทุจริตทางการเงิน เพื่อแลกเปลี่ยนและจัดเก็บข้อมูลที่เป็นประโยชน์ เช่น รูปแบบการทุจริต ข้อมูล blacklist หรือ watchlist ของบุคคลที่มีการทุจริต เป็นต้น เพื่อช่วยให้การป้องกัน การตรวจจับ การตอบสนองและรับมือภัยทุจริตมีประสิทธิภาพมากยิ่งขึ้น

(2.4.2) ร่วมกันสร้างความรู้และความตระหนักรู้ในการทำธุรกรรมทางการเงินแก่ประชาชนในลักษณะเชิงรุกและมีบูรณาการด้วยวิธีที่เกิดผลอย่างเป็นรูปธรรมในทางปฏิบัติ เพื่อให้ประชาชนเข้าใจและเพิ่มความระมัดระวังการทำธุรกรรมทางการเงิน

(2.4.3) กรณีเกิดเหตุการณ์ทุจริตจากการทำธุรกรรมทางการเงินต่อผู้ให้บริการทางการเงินหลายรายพร้อมกัน และส่งผลกระทบในวงกว้างต่อความเชื่อมั่นของระบบการเงินหรือระบบการชำระเงิน สมาคมธนาคารไทย สมาคมสถาบันการเงินแห่งรัฐ และสมาคมอื่นที่เกี่ยวข้อง ควรร่วมกันสื่อสารเพื่อชี้แจงและทำความเข้าใจกับผู้ใช้บริการอย่างรวดเร็ว และกำหนดแนวทางช่วยเหลือและเยียวยาผู้ใช้บริการให้เป็นมาตรฐานเดียวกัน รวมทั้ง ทบทวนและปรับปรุงแนวทางดังกล่าวอย่างต่อเนื่องด้วย

4. วันเริ่มต้นใช้

แนวนโยบายฉบับนี้ให้ใช้ตั้งแต่วันที่ 29 มีนาคม 2566 เป็นต้นไป

<u>เอกสารแนบ 1</u>

<u>การบริหารจัดการภัยทุจริตจากการทำธุรกรรมการชำระเงินผ่านบัตร</u>

ผู้ให้บริการทางการเงินที่เกี่ยวข้องกับการทำธุรกรรมการชำระเงินผ่านบัตร ต้องปฏิบัติเพิ่มเติมจากแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ดังนี้

1. การป้องกันภัย (Protection)

1.1 จัดให้มีการยืนยันตัวตนผู้ถือบัตรในการทำธุรกรรมการชำระเงินผ่านบัตร ครอบคลุมทั้งธุรกรรมการชำระเงินแบบ card present และ card not present สอดคล้องกับระดับความเสี่ยงของธุรกรรมและเป็นไปตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป เช่น การยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) เป็นต้น เพื่อให้มั่นใจว่าผู้ถือบัตรเป็นผู้ทำธุรกรรมที่เกิดขึ้นจริง

1.2 จัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลระหว่างการรับส่ง จัดเก็บหรือใช้ข้อมูลบัตรที่สอดคล้องตามมาตรฐานสากล เช่น มาตรฐาน The Payment Card Industry Data Security Standard (PCIDSS) รวมทั้งการนำเทคโนโลยีหรือวิธีการใหม่ ๆ มาใช้ยกระดับการรักษาความปลอดภัยในการทำธุรกรรม เช่น การใช้เทคโนโลยีสร้างเลขอ้างอิงเลขที่บัตร (tokenization) เป็นต้น

1.3 จัดให้มีระบบหรือช่องทางรองรับให้ผู้ถือบัตรสามารถบริหารจัดการความเสี่ยงในการทำธุรกรรมได้ด้วยตนเองในครั้งแรก อย่างน้อยครอบคลุม

(1) การเปิด-ปิดการทำธุรกรรมการชำระเงินที่ไม่ใช้บัตร โดยต้องตั้งค่าเริ่มต้น (default) เป็นปิดการทำธุรกรรมการชำระเงินที่ไม่ใช้บัตร

(2) กำหนดวงเงินสูงสุดในการทำธุรกรรมการชำระเงินผ่านบัตรต่อครั้ง และวงเงินสูงสุดต่อวัน

2. การตรวจจับ (Detection)

2.1 จัดให้มีระบบตรวจจับและติดตามความผิดปกติจากการทำธุรกรรมทางการเงินที่สามารถตรวจจับได้อย่างทันท่วงที (near real-time) และต่อเนื่องทั้งในและนอกเวลาทำการ (24x7)

2.2 กำหนดเงื่อนไขการตรวจจับอย่างน้อยครอบคลุม ธุรกรรมการชำระเงินที่ไม่ใช้บัตรที่ทำครั้งแรก ธุรกรรมที่ชำระด้วยเงินตราต่างประเทศ ธุรกรรมมูลค่าต่ำและความถี่สูง ธุรกรรมจากร้านค้าหรือกลุ่มบัตรที่มีความเสี่ยง เพื่อให้ครอบคลุมการทำธุรกรรมที่ผิดปกติและอาจเข้าข่ายการทำทุจริต โดยมีการทบทวนและปรับปรุงเงื่อนไขให้สอดคล้องกับระดับความเสี่ยงของภัยและของผู้ใช้บริการอย่างสม่ำเสมอ

3. การตอบสนองและรับมือ (Response)

3.1 เมื่อผู้ถือบัตรเกิดปัญหาจากการทำธุรกรรมการชำระเงินผ่านบัตร ซึ่งอาจก่อให้เกิดความเสียหายต่อผู้ถือบัตร ผู้ให้บริการทางการเงินที่เกี่ยวข้องกับการทำธุรกรรมการชำระเงินผ่านบัตร ต้องแจ้งการรับเรื่องให้กับผู้ถือบัตรทราบภายใน 1 ชั่วโมงนับจากได้รับแจ้งเหตุจากผู้ถือบัตร พร้อมทั้งแจ้งความคืบหน้าเบื้องต้นให้ผู้ถือบัตรทราบภายใน 1 วันทำการนับจากได้รับแจ้งจากผู้ถือบัตร

3.2 กรณีเหตุการณ์ทุจริตที่มีผู้ถือบัตรได้รับความเสียหายที่เกี่ยวข้องกับการทำธุรกรรมชำระเงินผ่านบัตร และมีเหตุอันเชื่อได้ว่าไม่ได้เกิดจากความผิดของผู้ถือบัตรหรือผู้ถือบัตรไม่มีส่วนเกี่ยวข้อง ผู้ให้บริการต้องเยียวยาความเสียหายให้กับผู้ถือบัตรอย่างครบถ้วน

(1) กรณีบัตรเดบิต ให้คืนเงินให้ผู้ถือบัตรตามยอดที่ถูกตัดชำระ โดยเร็วภายใน 5 วัน นับแต่วันที่ผู้ให้บริการพิจารณาแล้วมีเหตุอันเชื่อได้ว่าไม่ได้เกิดจากความผิดของผู้ถือบัตรหรือผู้ถือบัตรไม่มีส่วนเกี่ยวข้อง

(2) กรณีบัตรเครดิต ยกเลิกการเรียกเก็บรายการ โดยผู้ถือบัตรไม่ต้องชำระเงินและดอกเบี้ยที่เกิดขึ้น

4. ความร่วมมือ (Collaboration)

ผู้ให้บริการระบบเครือข่ายบัตรจัดให้มีมาตรการส่งเสริมและสนับสนุนให้สมาชิกเครือข่ายบัตรของตนอย่างชัดเจนและต่อเนื่อง อย่างน้อยครอบคลุม ดังนี้

4.1 การกำหนดแผนงานที่ชัดเจน เพื่อให้สมาชิกเครือข่ายบัตรยกระดับความมั่นคงปลอดภัยและระบบการบริหารจัดการความเสี่ยงจากการทำธุรกรรมการชำระเงินผ่านบัตร

4.2 การจัดให้มีระบบ กลไกและผู้รับผิดชอบในการประสานงานร่วมกับสมาชิกเครือข่ายบัตรในการช่วยเหลือให้สมาชิกสามารถป้องกัน ตรวจจับ ตอบสนองและรับมือภัยทุจริตได้ตามแนวทางข้างต้นได้อย่างเท่าทัน รวมทั้งสนับสนุนข้อมูลที่เป็นประโยชน์แก่สมาชิก เพื่อนำไปพัฒนาระบบการป้องกันและตรวจจับภัยให้มีประสิทธิภาพมากยิ่งขึ้น รวมทั้งประสานงานและร่วมมือเพื่อสร้างกลไกด้านความร่วมมือในการป้องกัน ติดตามตรวจจับ รับมือและแก้ไขเหตุการณ์ภัยทุจริตให้มีประสิทธิภาพมากยิ่งขึ้น

<u>เอกสารแนบ 2</u>

<u>การบริหารจัดการปัญหาการทุจริตและหลอกลวง</u>
<u>ผ่านการใช้บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์สำหรับผู้ใช้บริการรายย่อย</u>

ผู้ให้บริการทางการเงินที่ให้บริการเกี่ยวข้องกับบัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์เฉพาะที่ให้บริการโอนเงินไปยังบัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์ที่ให้บริการโดยผู้ให้บริการทางการเงินอื่นได้ (บัญชี e-Money ที่โอนเงินได้) สำหรับผู้ใช้บริการรายย่อย ต้องปฏิบัติเพิ่มเติมจากแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ดังนี้

1. การป้องกันภัย (Protection)

1.1 การเปิดบัญชีเงินฝากหรือบัญชี e-Money ที่โอนเงินได้ ให้ถือปฏิบัติตามหลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากหรือบัญชี e-Money เพื่อให้มั่นใจได้ว่าข้อมูลและเอกสารหลักฐานการแสดงตนของผู้ใช้บริการมีความถูกต้อง แท้จริงและเป็นปัจจุบัน รวมถึงสามารถพิสูจน์ได้ว่าผู้ใช้บริการที่ประสงค์จะเปิดบัญชีหรือเปิดใช้บริการ เป็นผู้ใช้บริการรายนั้นจริง รวมถึงให้ถือปฏิบัติตามกฎหมายและหลักเกณฑ์อื่นที่เกี่ยวข้องอย่างเคร่งครัด

สำหรับการเปิดบัญชีเงินฝากหรือบัญชี e-Money ที่โอนเงินได้ แบบไม่พบเห็นผู้ใช้บริการต่อหน้า (non-face-to-face) ทุกครั้ง ต้องมีวิธีการยืนยันตัวตนผู้ใช้บริการ (authenticate) ที่รัดกุมโดยใช้เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของผู้ใช้บริการ (biometric comparison) และเทคโนโลยี liveness detection เป็นขั้นต่ำ หรือใช้วิธีการอื่นที่เทียบเท่า เพื่อยืนยันตัวตนของผู้ทำธุรกรรมเปิดบัญชีและลดโอกาสการสวมรอยจากผู้ทำทุจริต

1.2 จัดให้มีการยืนยันตัวตนผู้ใช้บริการในขั้นตอนการทำธุรกรรมผ่านช่องทางให้บริการ mobile banking และช่องทางให้บริการ e-Money ที่โอนเงินได้ โดยใช้เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของผู้ใช้บริการ (biometric comparison) ซึ่งอาจพิจารณาเพิ่มเติมเทคโนโลยี liveness detection ร่วมด้วยตามความเหมาะสมหรือใช้วิธีการอื่นใดที่มีความรัดกุมเทียบเท่า เมื่อธุรกรรมดังกล่าวเป็นธุรกรรมที่เข้าเงื่อนไขอย่างใดอย่างหนึ่ง ดังนี้

(1) ทำธุรกรรมโอนเงินในแต่ละครั้งมีมูลค่า ตั้งแต่ 50,000 บาทขึ้นไป หรือ

(2) ทำธุรกรรมโอนเงิน มูลค่ารวมกัน ครบทุก ๆ 200,000 บาท ในรอบระยะเวลา 1 วัน หรือ

(3) ปรับเพิ่มวงเงินการทำธุรกรรมโอนเงินต่อวัน ให้สามารถโอนได้ตั้งแต่ 50,000 บาท ขึ้นไป

ทั้งนี้ หากการทำธุรกรรมข้างต้นเป็นธุรกรรมที่มีความเสี่ยงต่ำ เช่น การทำธุรกรรมโอนเงินระหว่างบัญชีตนเอง หรือการทำธุรกรรมโอนเงินประจำอัตโนมัติ (automatic recurring transfer) และได้ยืนยันตัวตนไปแล้วในครั้งแรก เป็นต้น อาจพิจารณางดเว้นการยืนยันตัวตนผู้ใช้บริการได้

ทั้งนี้ เงื่อนไขการทำธุรกรรมที่ต้องจัดให้มีการยืนยันตัวตนอาจเปลี่ยนแปลงได้ตามที่ ธปท. กำหนดเพื่อป้องกันการใช้บัญชีของบุคคลอื่นมาเป็นช่องทางในการกระทำความผิด ให้เท่าทันภัยทุจริตใหม่ ๆ และเพียงพอเหมาะสมกับรูปแบบการให้บริการทางการเงินในอนาคต

1.3 จัดให้มีกระบวนการพิสูจน์ความเป็นเจ้าของเลขหมายโทรศัพท์เคลื่อนที่ในขั้นตอนการเปิดบัญชีเงินฝาก การเปิดใช้บริการ mobile banking การเปิดบัญชี e-Money ที่โอนเงินได้ รวมทั้งเมื่อมี

การเปลี่ยนแปลงหมายเลขโทรศัพท์ โดยตรวจสอบให้ชื่อเจ้าของบัญชีเงินฝากหรือบัญชี e-Money ที่โอนเงินได้ตรงกันกับชื่อเจ้าของเลขหมายโทรศัพท์เคลื่อนที่ ทั้งนี้ กรณีที่ผู้ให้บริการทางการเงินไม่สามารถปฏิบัติได้จะต้องมีกระบวนการบริหารจัดการความเสี่ยงที่เพียงพอ เช่น พิสูจน์ได้ว่าเป็นการเปิดบัญชีเพื่อให้บุคคลในครอบครัวใช้งานหรือเปิดเพื่อใช้ในธุรกิจส่วนตัว เป็นต้น เพื่อป้องกันการนำหมายเลขโทรศัพท์เคลื่อนที่ของบุคคลอื่นมาใช้ในการเปิดใช้บริการ mobile banking หรือเปิดบัญชี e-Money ที่โอนเงินได้

1.4 กำหนดให้ผู้ใช้บริการสามารถเปิดใช้บริการ mobile banking หรือเปิดใช้บริการ e-Money ที่โอนเงินได้ ได้เพียง 1 บัญชีผู้ใช้งาน และจำกัดให้ใช้งานบน 1 อุปกรณ์เท่านั้น ทั้งนี้ หากผู้ให้บริการทางการเงินมีบริการ mobile banking หรือ บริการ e-Money ที่โอนเงินได้มากกว่า 1 แอปพลิเคชัน สามารถเปิดบัญชีผู้ใช้งานได้ตามจำนวนแอปพลิเคชัน

ทั้งนี้ ในกรณีที่ผู้ให้บริการทางการเงินอนุญาตให้ผู้ใช้บริการสามารถใช้ได้มากกว่า 1 อุปกรณ์ ผู้ให้บริการทางการเงินต้องสามารถติดตามและตรวจจับได้ว่าอุปกรณ์ถูกใช้งานจากผู้ใช้บริการจริง เช่น การติดตามจากอุปกรณ์ สถานที่ และพฤติกรรมในการทำธุรกรรม ของผู้ใช้บริการที่อาจผิดปกติไปจากเดิม เป็นต้น เพื่อป้องกันการสวมรอยทำธุรกรรมจากมิจฉาชีพ

1.5 กำหนดเพดานวงเงินสูงสุดต่อวันสำหรับธุรกรรมถอนเงินหรือโอนเงินในช่องทางการทำธุรกรรมต่าง ๆ ให้เหมาะสมตามความระดับเสี่ยงของกลุ่มผู้ใช้บริการแต่ละประเภท เพื่อลดความเสียหายเมื่อกลุ่มผู้ใช้บริการเหล่านี้ตกเป็นเหยื่อหรือถูกใช้เป็นเครื่องมือในการทำทุจริต ทั้งนี้ กรณีกลุ่มผู้ใช้บริการที่อายุต่ำกว่า 15 ปี ให้กำหนดวงเงินของช่องทางให้บริการทางอุปกรณ์เคลื่อนที่ (mobile banking) ช่องทางให้บริการทางอินเทอร์เน็ต (internet banking) ช่องทางสาขาอิเล็กทรอนิกส์ และช่องทางให้บริการ e-Money สูงสุดช่องทางละไม่เกิน 50,000 บาทต่อวัน

1.6 งดเว้นแนบลิงก์ทุกประเภทผ่านช่องทางข้อความสั้น (SMS) และช่องทางอีเมล สำหรับกรณีช่องทางโซเชียลมีเดียงดเว้นแนบลิงก์เฉพาะที่เป็นการขอข้อมูลในการยืนยันตัวตนและข้อมูลสำคัญส่วนบุคคลที่สำคัญ เช่น ชื่อผู้ใช้งาน รหัสผ่าน รหัส OTP รหัส PIN หมายเลขบัตรประชาชนชน วันเดือนปีเกิด เป็นต้น ทั้งนี้ ยกเว้นกรณีผู้ใช้บริการดำเนินการร้องขอเองเป็นรายครั้งสามารถแนบลิงก์ได้ทั้ง 3 ช่องทาง เพื่อป้องกันการแอบอ้างจากมิจฉาชีพสวมรอยเป็นผู้ให้บริการทางการเงินและหลอกขอข้อมูล (social engineering) หรือหลอกลวงให้ทำธุรกรรมทางการเงิน รวมทั้งสื่อสารเน้นย้ำกับผู้ใช้บริการทราบว่าผู้ให้บริการทางการเงินไม่มีนโยบายส่งลิงก์หรือให้ผู้ใช้บริการทำธุรกรรมทางการเงินใด ๆ ผ่านช่องทางดังกล่าว

1.7 ปรับปรุงระบบการรักษาความมั่นคงปลอดภัยการให้บริการ mobile banking และการให้บริการ e-Money ที่โอนเงินได้ ให้เป็นไปตามมาตรฐานสากลและหลักเกณฑ์ของ ธปท. รวมถึงเท่าทันภัยคุกคามรูปแบบใหม่อยู่เสมอ โดยผู้ให้บริการทางการเงินต้องเร่งดำเนินการปิดช่องโหว่โดยเร็วตามระดับความเสี่ยงหรือดำเนินการให้แล้วเสร็จภายในระยะเวลาที่ ธปท. กำหนด เพื่อให้มั่นใจว่าสามารถป้องกันภัยคุกคามรูปแบบใหม่ ๆ ได้อย่างทันกาล

1.8 จัดให้มีการประเมินความตระหนักรู้ต่อภัยทุจริต (awareness test) เมื่อผู้ใช้บริการเริ่มต้นใช้บริการ mobile banking และบริการ e-Money ที่โอนเงินได้ ครั้งแรก และประเมินอย่างต่อเนื่องทุก ๆ 6 เดือน เป็นขั้นต่ำ เพื่อสร้างความตระหนักรู้ต่อภัยทุจริต และเพิ่มภูมิคุ้มกันต่อรูปแบบการหลอกลวงใหม่ ๆ โดยอาจพิจารณานำผลการประเมินไปใช้ประกอบมาตรการป้องกันภัยทุจริตอื่นให้มีประสิทธิภาพยิ่งขึ้น เช่น

ใช้เป็นปัจจัยเพิ่มเติมในการกำหนดระดับความเสี่ยงของผู้ใช้บริการ การกำหนดความเข้มข้นในการสร้างความตระหนักรู้ หรือกำหนดค่าเริ่มต้นของวงเงินทำธุรกรรมต่อวัน เป็นต้น

2. การตรวจจับ (Detection)

2.1 จัดให้มีระบบตรวจจับและติดตามธุรกรรมที่เข้าข่ายผิดปกติ ที่สามารถตรวจจับได้อย่างทันท่วงที (near real-time) และต่อเนื่องทั้งในและนอกเวลาทำการ (24x7) และดำเนินการระงับธุรกรรมทันทีเป็นการชั่วคราวเมื่อตรวจพบ

2.2 กำหนดเงื่อนไขการตรวจจับและติดตามธุรกรรมที่เข้าข่ายผิดปกติ และจัดให้มีการทบทวนและปรับปรุงเงื่อนไขอย่างสม่ำเสมอ ครอบคลุม การใช้บัญชีเงินฝาก หรือบัญชี e-Money ที่โอนเงินได้ ของบุคคลอื่นมาเป็นช่องทางในการรับเงินและถ่ายโอนเงินที่ได้มาจากการกระทำความผิด (บัญชีม้า) โดยมีเงื่อนไขอย่างน้อยดังนี้

(1) ธุรกรรมโอนเงินที่มีลักษณะการใช้งานที่ผิดปกติ เช่น ธุรกรรมที่มีความถี่สูง
(2) ธุรกรรมที่มีการโอนเงินไปยังบัญชีเงินฝาก หรือบัญชี e-Money ต้องสงสัย
(3) บัญชีที่ปกติไม่มีการเคลื่อนไหว แต่เกิดการโอนเงินออกผิดปกติ
(4) บัญชีที่มีการโอนเงินเข้ามาจำนวนมากโดยโอนเข้ามาจากหลายบัญชีแต่โอนออกไปยังบัญชีปลายทางเพียงไม่กี่บัญชี
(5) บัญชีที่มีปริมาณเงินโอนเข้าและออกจำนวนมากแต่ใช้ระยะเวลาสั้น ๆ รวมถึงไม่มีเงินคงค้างในบัญชี (clear out)
(6) บัญชีที่มีปริมาณเงินโอนเข้าและออกผิดปกติ เช่น ไม่สอดคล้องกับวัตถุประสงค์การเปิดบัญชี รายได้ และอาชีพ เป็นต้น
(7) บัญชีที่มีการโอนเงินเข้าและออกมูลค่าน้อยในระยะเวลาสั้น ๆ หลายครั้งก่อนมีการโอนเงินยอดสูงและโอนออกไปทันที

นอกจากนี้ ผู้ให้บริการทางการเงินที่ตรวจพบบัญชีม้าหรือการหลอกลวงจำนวนมาก อาจพิจารณากำหนดเงื่อนไขเพิ่มเติม เช่น

(8) บัญชีที่ถูกยืนยันตัวตนอย่างกระจุกตัวเพื่อเปิดบัญชีในสถานที่ใดสถานที่หนึ่ง เช่น ตู้ ATM ที่ใช้ยืนยันตัวตนจำนวนมากในช่วงเวลาหนึ่ง เป็นต้น
(9) บัญชีหลายบัญชี (ต่างบุคคล) ที่ใช้หมายเลขโทรศัพท์เดียวกัน ในการเปิดบัญชีหรือทำธุรกรรม
(10) บัญชีที่มีการทำธุรกรรมจากต่างสถานที่ในระยะเวลาใกล้เคียงกัน หรือจากสถานที่ต้องสงสัยว่าเป็นแหล่งอาชญากรรม
(11) บัญชีกลุ่มเปราะบางที่อาจถูกหลอกลวง เช่น ผู้ใช้บริการที่อายุต่ำกว่า 15 ปี หรือผู้สูงวัย

3. การตอบสนองและรับมือ (Response)

3.1 จัดให้มีช่องทางติดต่อเร่งด่วน (hotline) ทางโทรศัพท์ หรือวิธีการทางอิเล็กทรอนิกส์ที่ผู้ใช้บริการสามารถติดต่อได้โดยตรงแยกออกจากช่องทางให้บริการปกติ อย่างเพียงพอและต่อเนื่องทั้งในและนอกเวลาทำการ (24x7) เพื่อให้ผู้ใช้บริการสามารถแจ้งเหตุภัยทุจริตจากการทำธุรกรรมทางการเงินได้โดยเร็ว

ทั้งนี้ หลังได้รับแจ้งเหตุ ผู้ให้บริการทางการเงินต้องเร่งดำเนินการตามกฎหมายและหลักเกณฑ์อื่นที่เกี่ยวข้องอย่างเคร่งครัด เพื่อลดความเสียหายที่อาจเกิดขึ้น

3.2 เมื่อผู้ให้บริการทางการเงินตรวจสอบพบบัญชีที่มีลักษณะเข้าข่ายกรณีบัญชีม้าให้รายงานเป็นธุรกรรมที่มีเหตุอันควรสงสัยไปยังสำนักงานป้องกันและปราบปรามการฟอกเงิน (สำนักงาน ปปง.) หรือกรณีได้รับแจ้งจากสำนักงาน ปปง. ให้ดำเนินการจำกัดช่องทางการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยกำหนดให้ทำธุรกรรมแบบพบหน้าเท่านั้น พิจารณาปรับระดับความเสี่ยงของผู้ใช้บริการเป็นผู้ใช้บริการที่มีความเสี่ยงสูง ตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าในระดับเข้มข้น (enhanced CDD) โดยให้เพิ่มความระมัดระวังในการสร้างความสัมพันธ์ เฝ้าระวังการทำธุรกรรมอย่างใกล้ชิด ทั้งนี้ หากผู้ให้บริการทางการเงินไม่สามารถดำเนินการ enhanced CDD ได้ ให้กำหนดมาตรการในการปฏิเสธความสัมพันธ์ทางธุรกิจ ไม่ทำธุรกรรม หรือยุติความสัมพันธ์ และหากพบว่ามีการทำธุรกรรมมีเหตุอันควรสงสัย ให้ผู้ให้บริการทางการเงินพิจารณารายงานธุรกรรมที่มีเหตุอันควรสงสัยไปยังสำนักงาน ปปง. เพื่อลดการนำบัญชีไปใช้เป็นเครื่องมือทำทุจริตและจำกัดความเสียหายจากการหลอกลวง

ทั้งนี้ มาตรการดังกล่าวเป็นเพียงแนวทางในการดำเนินการ ให้ผู้ให้บริการถือปฏิบัติตามกฎกระทรวงว่าด้วยการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า รวมถึงประกาศ หลักเกณฑ์ และแนวปฏิบัติอื่น ๆ ที่เกี่ยวข้องตามที่สำนักงาน ปปง. และกฎหมายอื่นที่เกี่ยวข้องกำหนด

3.3 ดำเนินการ ระงับ อายัด จำกัดวงเงิน โดยทันที ตามที่ระบุในหนังสือคำสั่งจากพนักงานสอบสวน เพื่อสกัดกั้นการนำเงินออกจากระบบของมิจฉาชีพและจำกัดความเสียหายในกรณีผู้ใช้บริการถูกหลอกลวงหรือแอบอ้างทำธุรกรรมทางการเงิน รวมทั้งดำเนินการตามที่กฎหมายอื่นที่เกี่ยวข้องกำหนด

3.4 จัดให้มีกลไกการสื่อสารทั้งกับหน่วยงานภายในที่เกี่ยวข้อง เช่น call center และหน่วยงานภายนอก โดยกำหนดระยะเวลาในการสื่อสารให้ชัดเจนตามระดับความสำคัญ เพื่อให้สามารถตอบสนองได้อย่างทันกาล และสร้างความเชื่อมั่นต่อสาธารณะ

3.5 กรณีที่มีความเสียหายเกิดขึ้นจากภัยทุจริตจากการทำธุรกรรมทางการเงิน ให้ผู้ให้บริการทางการเงินช่วยเหลือและดูแลผู้ใช้บริการตามสมควร และหากมีเหตุอันควรเชื่อได้ว่าความเสียหายดังกล่าวเกิดจากความผิดพลาดหรือบกพร่องของผู้ให้บริการทางการเงิน ผู้ให้บริการทางการเงินต้องเยียวยาความเสียหายอย่างเป็นธรรมและเหมาะสมให้กับผู้ใช้บริการโดยเร็วซึ่งจะต้องไม่เกิน 5 วันนับแต่วันที่ผู้ให้บริการทางการเงินพิสูจน์ทราบความผิดพลาดหรือบกพร่องดังกล่าว

4. ความร่วมมือ (Collaboration)

4.1 ให้การสนับสนุนข้อมูลให้แก่พนักงานสอบสวนที่ได้รับมอบหมายจากระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติโดยเร็ว หรือแก่พนักงานสอบสวนที่เกี่ยวข้องเมื่อถูกร้องขออย่างทันกาล เพื่อใช้ในการสืบสวนสอบสวนและติดตามหาผู้กระทำผิด โดยจัดให้มีผู้รับผิดชอบในการดูแลและประสานงานกับหน่วยงานต่าง ๆ อย่างชัดเจน และให้จัดเตรียมข้อมูลอย่างน้อยครอบคลุมในเรื่องดังต่อไปนี้

(1) หมายเลข IP address ที่ใช้ในการทำธุรกรรม

(2) ข้อมูลการทำธุรกรรม เช่น เลขบัญชีปลายทาง ชื่อผู้รับหรือชื่อบัญชีปลายทาง เป็นต้น

(3) ข้อมูลเชิงเทคนิคของอุปกรณ์ที่ใช้ทำธุรกรรม เช่น OS version, MAC address, device ID, mobile application version, browser version, IMEI number และหมายเลขโทรศัพท์ของอุปกรณ์ที่ใช้ทำธุรกรรม (MSISDN) เป็นต้น

4.2 สนับสนุนหน่วยงานของรัฐที่เกี่ยวข้องในการสื่อสารแก่ประชาชนผ่านช่องทางที่เข้าถึงได้ง่าย เพื่อสร้างความตระหนักรู้ในวงกว้าง และป้องกันไม่ให้ประชาชนตกเป็นเหยื่อของการหลอกลวงรูปแบบใหม่ ๆ โดยมีข้อความแจ้งเตือนภัยทุจริตและหลอกลวงออนไลน์ต่าง ๆ ที่เด่นชัดและสังเกตเห็นได้ง่าย ก่อนการทำธุรกรรมทุกครั้งผ่านช่องทางให้บริการ mobile banking หรือช่องทางให้บริการ e-Money ที่โอนเงินได้

คำถาม – คำตอบแนบท้ายแนวนโยบาย

เรื่อง การบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน

ลำดับ	ประเด็นคำถาม	แนวคำตอบ
1	ขอทราบขอบเขตและแนวทางการบังคับใช้	แนวนโยบายฉบับนี้บังคับใช้กับสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน รวมถึงผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน เจตนาต้องการให้ผู้ให้บริการทางการเงินมีแนวทางการบริหารจัดการภัยทุจริตที่ครอบคลุมการทำธุรกรรมทางการเงินตามนิยามที่กำหนด ทั้งนี้ สำหรับกรณีการทำธุรกรรมชำระเงินผ่านบัตร และการให้บริการที่เกี่ยวข้องกับบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์เฉพาะที่ให้บริการโอนเงินไปยังบัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์ที่ให้บริการโดยผู้ให้บริการทางการเงินอื่นได้ สำหรับผู้ใช้บริการรายย่อย ให้ปฏิบัติเพิ่มเติมตามเอกสารแนบด้วย
2	ความเสียหายต่อผู้ใช้บริการในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของผู้ให้บริการทางการเงิน พิจารณาอย่างไร	ให้พิจารณาผลกระทบ ดังนี้ (1) ผลกระทบต่อลูกค้าจำนวนมาก (2) ผลกระทบต่อระบบการเงินและการชำระเงิน เช่น กระทบต่อผู้ให้บริการหลายราย กระทบต่อระบบงานกลางที่มีนัยสำคัญ เป็นต้น (3) ผลกระทบต่อชื่อเสียงของผู้ให้บริการ เช่น มูลค่าความเสียหายจำนวนสูง เป็นต้น
3	การรายงานเหตุการณ์ทุจริตที่ก่อให้เกิดความเสียหายกับผู้ใช้บริการในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของผู้ให้บริการทางการเงิน ให้ ธปท. ทราบโดยเร็วตามช่องทางที่กำหนด ธปท. หมายถึงช่องทางใด	เจตนาต้องการให้แจ้งผู้ประสานงาน ธปท. (เจ้าหน้าที่สัมพันธ์: relationship manager) ทันทีผ่านระบบ event report ทั้งนี้ ผู้ให้บริการยังคงต้องจัดทำรายงานตามรอบให้เป็นไปตามกฎเกณฑ์อื่น ๆ ที่กำหนดไว้ด้วย
เอกสารแนบ 1 การบริหารจัดการภัยทุจริตจากการทำธุรกรรมการชำระเงินผ่านบัตร		
4	ธุรกรรมการชำระเงินผ่านบัตร ตามเอกสารแนบ 1 นั้นรวมกรณี card present หรือไม่	เอกสารแนบ 1 ใช้กับการทำธุรกรรมการชำระเงินผ่านบัตร ทั้งกรณี card present และ not present

5	กรณีที่ e-wallet มีการผูกบัตรเครดิต/เดบิต โดยมีการยืนยันตัวตนผ่านแล้ว สามารถทำธุรกรรมการชำระสินค้า/บริการได้เลยหรือไม่	ในการทำธุรกรรม ผู้ให้บริการทางการเงินยังต้องจัดให้มีการยืนยันตัวตนผู้ถือบัตรให้สอดคล้องกับระดับความเสี่ยงของธุรกรรมด้วย แม้ว่าจะมีการยืนยันตัวตนในขั้นตอนการผูกบัตรแล้วก็ตาม เนื่องจากยังมีความเสี่ยงที่อาจเกิดภัยทุจริตได้
6	ขอทราบตัวอย่างข้อมูล ที่ใช้ในการประเมินความเสี่ยงของธุรกรรม	ตัวอย่างข้อมูล เช่น currency, purchase amount, IP address, browser, time zone, frequency, merchant risk indicator เป็นต้น ซึ่งเป็นไปตามหลักการทำ enhanced authentication data (EMV 3DS) ของผู้ประกอบธุรกิจระบบเครือข่ายบัตร
7	การแจ้งการรับเรื่องให้กับผู้ถือบัตรทราบภายใน 1 ชั่วโมงนับจากได้รับแจ้งเหตุจากผู้ถือบัตร ธปท. คาดหวังการติดต่อกลับแบบใด	ผู้ให้บริการทางการเงินสามารถติดต่อกลับลูกค้าได้ในทุกช่องทางที่ผู้ให้บริการได้จัดเตรียมไว้ เพื่อให้ลูกค้าได้รับการช่วยเหลือโดยเร็วและสามารถดำเนินการเพื่อลดความเสียหายที่อาจเกิดขึ้นกับตนได้
เอกสารแนบ 2 การบริหารจัดการปัญหาการทุจริตและหลอกลวง ผ่านการใช้บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์สำหรับผู้ใช้บริการรายย่อย		
8	กรณี ลูกค้าชาวต่างชาติ ลูกค้าสามารถใช้เอกสารหลักฐานใดเป็นเอกสารหลักฐานการแสดงตน และจัดเก็บรูปหน้า	ลูกค้าชาวต่างชาติสามารถใช้เอกสารหลักฐานการแสดงตน ตามที่กำหนดในหลักเกณฑ์ของกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินที่ใช้บังคับอยู่ในปัจจุบัน เช่น ข้อมูลอิเล็กทรอนิกส์ที่ได้จากหนังสือเดินทาง เช่น ข้อมูลจากเทคโนโลยีสื่อสารไร้สายระยะใกล้ (NFC) และตรวจสอบเอกสารสำคัญประจำตัวอื่นที่รัฐบาลไทยออกให้หรือหน่วยงานของรัฐเจ้าของสัญชาติออกให้ หรือใช้วิธีการอื่นใดที่มีระดับความน่าเชื่อถือเทียบเคียงกัน
9	ขอทราบขอบเขตประเภทธุรกรรมที่เข้าข่ายต้องยืนยันตัวตนด้วย biometric comparison (โอนเงิน/โอนเงินผ่าน QR code/ธุรกรรมชำระเงิน/ซื้อกองทุน/เติมเงิน)	กรอบหลักการของมาตรการนี้ เพื่อให้ยืนยันตัวตนผู้ใช้บริการในการทำธุรกรรมที่มีความเสี่ยงสูง และมีโอกาสถูกหลอกทำธุรกรรมไปยังมิจฉาชีพ จึงกำหนดครอบคลุมธุรกรรมโอนเงินภายในธนาคารและต่างธนาคาร รวมทั้งการโอนเงินผ่าน QR code อย่างไรก็ตาม ไม่นับรวม ธุรกรรมชำระเงิน ธุรกรรมชำระซื้อกองทุน และการเติมเงิน เนื่องจากมีกระบวนการป้องกัน เช่น KYM ทำให้มีความเสี่ยง

		ต่ำกว่า และไม่ใช่ช่องทางหลักที่มิจฉาชีพใช้ในการหลอกลวงเหยื่อ หรือช่องทางการใช้บัญชีม้า
10	ถ้าลูกค้าเป็นฝ่ายติดต่อขอข้อมูลมายังผู้ให้บริการทางการเงิน สามารถส่ง SMS หรืออีเมลที่มีลิงก์แนบได้หรือไม่	หากลูกค้าเป็นผู้ร้องขอให้ผู้ให้บริการทางการเงินส่งข้อมูลมาผ่านช่องทาง SMS หรืออีเมล ผู้ให้บริการทางการเงินสามารถส่งลิงก์ผ่าน SMS หรืออีเมลแก่ลูกค้าได้ ทั้งนี้ ขอให้สื่อสารให้ลูกค้าใช้ความระมัดระวังในการสังเกตรายละเอียดข้อมูลและแหล่งที่มาของข้อมูลก่อนคลิกลิงก์ทุกครั้ง
11	สามารถส่งลิงก์ URL website หลักของผู้ให้บริการทางการเงิน หรือ URL ที่เป็นข้อความไม่สามารถคลิกได้ หรือ QR code ผ่านช่องทาง SMS และอีเมล ได้หรือไม่	เพื่อป้องกันประชาชนตกเป็นเหยื่อของมิจฉาชีพ ให้ผู้บริการทางการเงินงดส่ง link ทุกประเภท ซึ่งรวมถึง QR code และข้อความในลักษณะ URL ผ่านช่องทางดังกล่าวด้วย โดย ธปท. จะสื่อสารเน้นย้ำกับประชาชนว่าผู้ให้บริการทางการเงินไม่มีนโยบายส่ง Link ผ่านช่องทาง SMS และ อีเมล
12	การตรวจสอบความเป็นเจ้าของหมายเลขโทรศัพท์เคลื่อนที่บัญชีเงินฝากหรือบริการ e-Money ตรงกันกับเจ้าของเลขหมายโทรศัพท์เคลื่อนที่นั้นสามารถทำโดยวิธีการใด และหากพบความไม่ตรงกันควรทำอย่างไร	การตรวจสอบความเป็นเจ้าของหมายเลขโทรศัพท์เคลื่อนที่ทำได้หลายวิธี เช่น - ผ่านระบบ USSD บนโทรศัพท์เคลื่อนที่ โดยให้ผู้ใช้บริการกด *179* + “หมายเลขบัตรประชนตนเอง 13 หลัก” + # และกดโทรออก - ผ่านระบบ mobile ownership validation ของบริษัท NITMX - ตรวจสอบกับบริษัทผู้ให้บริการโทรศัพท์เคลื่อนที่โดยตรง ในกรณีที่ไม่สามารถพิสูจน์ความเป็นเจ้าของหมายเลขโทรศัพท์เคลื่อนที่หรือพบความไม่สอดคล้องของชื่อ ให้ใช้กระบวนการบริหารจัดการความเสี่ยงที่เพียงพอรองรับ เช่น พิสูจน์ได้ว่าเป็นการเปิดบัญชีเพื่อให้บุคคลในครอบครัวใช้งานหรือเปิดเพื่อใช้ในธุรกิจส่วนตัว เป็นต้น หรือผู้ให้บริการอาจพิจารณาขอสงวนสิทธิ์การให้บริการตามระดับความเสี่ยงที่ยอมรับได้
13	จากข้อกำหนดเรื่องการบริหารความเสี่ยงจากการให้ใช้มากกว่า 1 อุปกรณ์ ซึ่งต้องสามารถติดตามและตรวจจับได้ว่าเจ้าของเป็นคนใช้งานจริง เช่น	มาตรการดังกล่าวมีวัตถุประสงค์เพื่อป้องกันมิจฉาชีพลักลอบเข้าถึงอุปกรณ์ของผู้ใช้งานได้โดยไม่ได้รับอนุญาต ดังนั้น หากผู้ให้บริการอนุญาตให้ลง mobile application มากกว่า 1 อุปกรณ์

	ติดตามจากอุปกรณ์ สถานที่ และพฤติกรรม ในการทำธุรกรรมของลูกค้าที่อาจผิดปกติไปจากเดิม เป็นต้น หากมีการพิสูจน์ตัวตนโดยใช้ biometric comparison และ liveness detection ผ่าน แต่ไม่สามารถเข้าถึงข้อมูล location หรือ behavior ของการใช้โทรศัพท์ของลูกค้าได้ เนื่องจากลูกค้าไม่อนุญาต กรณีดังกล่าวผู้ให้บริการจะยังสามารถให้บริการได้หรือไม่	จะต้องจัดให้มีกระบวนการพิสูจน์ตัวตนและการติดตามได้ว่าเป็นผู้ใช้งานตัวจริง ทั้งนี้หากมีบางปัจจัยในการติดตามอาจไม่สามารถใช้ได้ เนื่องด้วยเรื่องข้อจำกัดด้านกฎหมายหรือข้อจำกัดด้านอื่น ผู้ให้บริการสามารถพิจารณาใช้ปัจจัยอื่น ๆ ที่เหมาะสมทดแทนได้ เช่น การเข้าใช้งานจาก IP Address ที่มาจากต่างประเทศ พฤติกรรมการเงินที่ผิดปกติ เป็นต้น
14	จากข้อกำหนดเรื่องให้การสนับสนุนข้อมูลให้แก่พนักงานสอบสวนที่ได้รับมอบหมายจากระบบแจ้งความออนไลน์ ของสำนักงานตำรวจแห่งชาติโดยเร็ว หรือแก่พนักงานสอบสวน ที่เกี่ยวข้อง เมื่อถูกร้องขออย่างทันการณ์นั้น พนักงานสอบสวนจะส่งหนังสือคำสั่งมาให้เช่นเดิมใช่หรือไม่	กระบวนการส่งหนังสือคำสั่งยังคงปฏิบัติตามเดิม มาตรการดังกล่าวเป็นการจัดเตรียมความพร้อมของข้อมูลเพื่อสนับสนุนให้แก่พนักงานสอบสวนโดยเร็ว