ธนาคารแห่งประเทศไทย
BANK OF THAILAND

[ร่าง] หลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล [Digital Fraud Management]

ธนาคารแห่งประเทศไทย

4 มีนาคม 2568

กรอบหลักเกณฑ์ Digital Fraud Management

Intended Outcome ผู้ให้บริการมีกระบวนการป้องกัน ตรวจจับ และรับมือกับภัยทุจริตดิจิทัล

หลักการ Digital Fraud Management

ต้องดำเนินการอย่างเหมาะสมและทันกาล โดยต้องสร้างความสมดุลระหว่างความสะดวกและความปลอดภัย ในการทำธุรกรรมทางการเงิน และคำนึงถึงการคุ้มครองลูกค้าอย่างเป็นธรรม

Governance คณะกรรมการและผู้บริหารระดับสูงให้ความสำคัญกับ Digital Fraud Management และมีนโยบายที่สอดคล้องกับ Industry Standards ซึ่งได้ผ่านการหารือกับ ธปท. แล้ว

ตรวจจับภัยทุจริตดิจิทัล	จัดการภัยทุจริตดิจิทัล	แก้ไขหลังเกิดภัยทุจริตดิจิทัล
1 การรู้จักลูกค้า (KYC/CDD/EDD) "ประเมินความเสี่ยงของลูกค้า"	3 การบริหารจัดการภัยทุจริตทางการเงิน (Action) "ป้องกัน จำกัด ระงับความเสียหาย"	4 การแก้ไขปัญหาและดูแลลูกค้า (Response) "ชัดเจน รวดเร็ว เป็นธรรม"
2 การประเมินและติดตามความเสี่ยง (Monitoring) "ตรวจจับและติดตาม ความผิดปกติ รวมถึงมีกระบวนการติดตามและปรับปรุงสม่ำเสมอ"	ป้องกันเหยื่อ "เตือนและหน่วง" / จัดการม้า "ระงับธุรกรรม"	

Enabler

- **กระบวนการแลกเปลี่ยนข้อมูล** "ระบบ CFR + แชร์เส้นเงินไปตำรวจติดตามม้าได้รวดเร็ว"
- **ส่งเสริมความรู้ทางการเงิน** "ประชาชนไม่ตกเป็นเหยื่อมิจฉาชีพ"

ขอบเขตการบังคับใช้

ผู้ให้บริการทางการเงิน • ธนาคารพาณิชย์ • SFIs ที่รับฝากเงินจากประชาชน • E-money ที่โอนเงินได้	**ทำตามประกาศทุกข้อ**
ผู้ให้บริการทางการเงินอื่น • บริษัทเครดิตฟองซิเอร์ • บริษัทเงินทุน • ผู้ประกอบธุรกิจระบบการชำระเงิน • ผู้ประกอบธุรกิจบริการการชำระเงิน	**ปรับใช้ตามความเหมาะสม** ทั้งนี้ ให้ขึ้นกับขอบเขตการประกอบธุรกิจ ประเภทของผลิตภัณฑ์ และช่องทางการให้บริการ

1 การกำหนดนโยบายและการกำกับดูแล การบริหารจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

คณะกรรมการและผู้บริหารระดับสูงของผู้ให้บริการทางการเงินต้องกำกับดูแลให้ผู้ให้บริการทางการเงินมีการบริหารจัดการเหตุการณ์ภัยทุจริตดิจิทัลที่เหมาะสมกับรูปแบบและผลกระทบของภัยทุจริตดิจิทัลที่เกิดขึ้น และมีการแก้ไขสถานการณ์ที่ทันกาล เพื่อป้องกันและลดความเสียหายที่จะเกิดขึ้นกับประชาชน ตั้งแต่ต้นจนจบกระบวนการ (end-to-end)

1. **กำหนดให้มีคณะกรรมการหรือผู้บริหารระดับสูง**ที่ได้รับมอบหมายทำหน้าที่กำหนดนโยบายและกำกับดูแลอย่างชัดเจน

2. **กำหนดนโยบายการบริหารจัดการภัยทุจริตดิจิทัล**ที่ชัดเจน สอดคล้องกับกฎหมายที่เกี่ยวข้อง และ Industry Standards ครอบคลุม
   - บทบาทหน้าที่ของคณะกรรมการหรือผู้บริหารระดับสูง
   - แนวทางและกระบวนการบริหารจัดการภัยทุจริตดิจิทัลแบบ end-to-end
   - การติดตามและวัดประสิทธิผลของการจัดการภัยทุจริตดิจิทัลอย่างต่อเนื่อง

3. **กำหนดเป้าหมายและตัวชี้วัดในการประเมินประสิทธิผล**

4. **ออกแบบและพัฒนา ระบบงาน กระบวนการ และผลิตภัณฑ์หรือบริการทางการเงิน** โดยคำนึงถึงเหตุการณ์และปัจจัยความเสี่ยงที่อาจทำให้เกิดภัยทุจริตดิจิทัล

5. **ติดตามและประเมินประสิทธิผล**ของการบริหารจัดการภัยทุจริตดิจิทัล รวมทั้งปรับปรุงระบบงาน กระบวนการ และผลิตภัณฑ์หรือบริการทางการเงิน ให้ครอบคลุมรูปแบบของภัยทุจริตที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง

6. **สนับสนุนการจัดทำมาตรฐานอุตสาหกรรม (Industry Standards)** โดยให้ครอบคลุมกระบวนการบริหารจัดการภัยทุจริตดิจิทัลที่จำเป็น

2 กระบวนการจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

(1) กระบวนการรู้จักลูกค้า (KYC) และการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (CDD)

การทำ KYC/CDD	• การประเมินความเสี่ยงที่ลูกค้าอาจเข้าข่ายเป็นบัญชีม้า • กำหนดกระบวนการรู้จักลูกค้าและการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าที่สอดคล้องกับระดับความเสี่ยงของลูกค้า • ติดตามและวิเคราะห์พฤติกรรมการทำธุรกรรมของลูกค้า รวมถึงทบทวนระดับความเสี่ยงของลูกค้าให้เป็นปัจจุบันอยู่เสมอ • ดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าในระดับเข้มข้น (enhanced CDD) กรณีลูกค้ามีความเสี่ยงสูง

2 กระบวนการจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

[2] การติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงิน [monitoring & detection]

ผู้ให้บริการทางการเงินต้องมีกระบวนการในการติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงินที่มีประสิทธิผลและเป็นลักษณะเชิงรุก ครอบคลุมรูปแบบของภัยทุจริตดิจิทัลที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง โดยต้องสามารถประเมินระดับความเสี่ยงของบัญชีทั้งบัญชีของบุคคลที่คาดว่าจะได้รับความเสียหายและบุคคลที่มีความเสี่ยงเป็นบัญชีม้า รวมถึงตรวจจับธุรกรรมและบัญชีที่มีความผิดปกติได้อย่างทันท่วงที

1. **จัดให้มีบุคลากร กระบวนการ และระบบ**ในการติดตามและตรวจจับความผิดปกติจากการทำธุรกรรมทางการเงินอย่างเพียงพอเหมาะสม
2. **กำหนดเงื่อนไขในการติดตามและตรวจจับ**ความผิดปกติ ทั้งธุรกรรมของ**บุคคลที่คาดว่าจะได้รับความเสียหายและบุคคลที่มีความเสี่ยงเป็นบัญชีม้า** โดยต้องพิจารณาถึงปัจจัยต่าง ๆ ดังนี้
   - **รูปแบบของภัยทุจริตดิจิทัลที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง** ทั้งที่เกิดขึ้นภายในประเทศไทยและในต่างประเทศ
   - **ช่องทางการให้บริการ** เช่น สาขาทั่วไป สาขาอิเล็กทรอนิกส์ และช่องทางดิจิทัล
   - **ข้อมูลของลูกค้า**ที่สามารถใช้ประเมินความเสี่ยงและความผิดปกติของธุรกรรม เช่น ยอดเงินฝากในบัญชี พฤติกรรมการใช้บัญชี ข้อมูลพฤติกรรมต้องสงสัยที่ผู้ให้บริการทางการเงินตรวจพบเอง ข้อมูลเจ้าของหมายเลขโทรศัพท์เคลื่อนที่ ข้อมูลที่สามารถระบุพิกัดหรือตำแหน่งการทำธุรกรรมของลูกค้า และข้อมูลเชิงเทคนิคของอุปกรณ์ที่ใช้ทำธุรกรรม
   - **ข้อมูลจากภายนอก** เช่น ข้อมูลที่ได้รับจากผู้ให้บริการทางการเงินแห่งอื่น ข้อมูลจากระบบ Central Fraud Registry (CFR) ข้อมูลจากสำนักงานป้องกันและปราบปรามการฟอกเงิน ข้อมูลจากสำนักงานตำรวจแห่งชาติ และข้อมูลจากแหล่งอื่น ๆ ที่น่าเชื่อถือ

2 กระบวนการจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

[3] การจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน [actions]

ผู้ให้บริการทางการเงินต้องมีกระบวนการป้องกัน จำกัด และระงับความเสียหายจากภัยทุจริตดิจิทัลอย่างรวดเร็ว เพียงพอและเหมาะสม สอดคล้องตามระดับความเสี่ยงของธุรกรรม

1. การป้องกันและจำกัดความเสียหายให้แก่ลูกค้า	<u>ตัวอย่างการจัดการเพื่อป้องกันและจำกัดความเสียหาย</u> • **การแจ้งเตือนลูกค้าแบบทันที (real time)** กรณีลูกค้าทำธุรกรรมที่มีความเสี่ยง เช่น การโอนเงินไปสู่บัญชีของบุคคลที่มีลักษณะหรือพฤติกรรมผิดปกติที่เข้าข่ายเป็นบัญชีม้าทุกประเภท • **การแจ้งเตือนการทำธุรกรรมผ่านช่องทางต่าง ๆ โดยไม่มีค่าใช้จ่าย** เช่น การแจ้งเตือนผ่าน LINE อีเมล SMS • **การหน่วงหรือระงับธุรกรรมเมื่อตรวจพบความผิดปกติในการเดินบัญชี** เช่น การโอนเงินออกเป็นจำนวนมากภายในระยะเวลาที่รวดเร็ว **(rapidly drained)** • **การหน่วงธุรกรรม (cooling off period)** กรณีมีการดำเนินการที่มีความเสี่ยงสูง เช่น การติดตั้ง mobile banking บนอุปกรณ์ใหม่ การโอนเงินครั้งแรกภายหลังการเปิดใช้บริการ mobile banking การเปลี่ยน password • การติดต่อหาลูกค้าเพื่อสอบถามผู้รับผลประโยชน์ที่แท้จริงและยืนยันการทำธุรกรรม **(call back)** <u>ตัวอย่างระบบรองรับให้ลูกค้าสามารถบริหารความเสี่ยงจากการใช้บริการ mobile banking</u> • การตั้งค่าบัญชีหรือเงินในบัญชีไม่ให้ทำธุรกรรมผ่านช่องทางอิเล็กทรอนิกส์ **(money lock)** • การระงับการใช้บริการ mobile banking ด้วยตนเอง **(kill switch)**

(ดำเนินการให้แล้วเสร็จภายใน มิ.ย. 68 หรือตามที่กำหนดใน Industry Standards)

2 กระบวนการจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

[3] การจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน [actions]

ผู้ให้บริการทางการเงินต้องมีกระบวนการป้องกัน จำกัด และระงับความเสียหายจากภัยทุจริตดิจิทัลอย่างรวดเร็ว เพียงพอและเหมาะสม สอดคล้องตามระดับความเสี่ยงของธุรกรรม

2. การจัดการบัญชีที่อาจเข้าข่ายเป็นบัญชีม้า เพื่อจำกัดและระงับความเสียหาย	**ตัวอย่างการจัดการบัญชีที่อาจเข้าข่ายเป็นบัญชีม้า** • การกำหนดวงเงินการทำธุรกรรมต่อวันให้เหมาะสมกับระดับความเสี่ยงของลูกค้า เช่น การตั้งค่าวงเงินเริ่มต้นของการทำธุรกรรมต่อวันของบริการ mobile banking • การระงับเงินเข้า การระงับเงินออก การระงับช่องทางอิเล็กทรอนิกส์ การปฏิเสธการสร้างความสัมพันธ์ เช่น การปฏิเสธการเปิดบัญชีใหม่ การไม่เสนอขายผลิตภัณฑ์อื่น ๆ

[ดำเนินการให้แล้วเสร็จภายใน มิ.ย. 68 หรือตามที่กำหนดใน Industry Standards]

2 กระบวนการจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

[4] การแก้ไขสถานการณ์และการดูแลลูกค้า [response]

ผู้ให้บริการทางการเงินต้องกำหนดกระบวนการแก้ไขสถานการณ์
และดูแลลูกค้าเมื่อเกิดเหตุการณ์ภัยทุจริตดิจิทัลที่ชัดเจน รวดเร็ว และเป็นธรรม

ช่องทางรับแจ้งเหตุ	ระยะเวลาการแก้ไขปัญหา [Service Level Agreement]	การช่วยเหลือและดูแลลูกค้า	รายงานเหตุการณ์ภัยทุจริต
มีช่องทางติดต่อเร่งด่วน [hotline] - ทางโทรศัพท์ หรือวิธีการทางอิเล็กทรอนิกส์ - แยกออกจากช่องทางให้บริการปกติ - เพียงพอและต่อเนื่องทั้งในและนอกเวลาทำการ [24x7]	**กำหนดระยะเวลาการแก้ไขปัญหาที่เหมาะสม** - การติดต่อกลับลูกค้าอย่างรวดเร็วภายในเวลาที่เหมาะสม - การช่วยเหลือและดูแลลูกค้า	**ช่วยเหลือและดูแลลูกค้าอย่างเหมาะสม รวดเร็ว และเป็นธรรม** - จัดการแก้ไขปัญหาที่รวดเร็ว เช่น ยกเลิกการหน่วงธุรกรรม การปลดการระงับบัญชี	**รายงานผู้บริหารและ ธปท.** - **กรณีความเสียหายไม่รุนแรง :** รายงานคณะกรรมการหรือผู้บริหารระดับสูง - **กรณีความเสียหายวงกว้างหรือกระทบชื่อเสียง :** รายงาน ธปท.

3 การแลกเปลี่ยนข้อมูลระหว่างผู้ให้บริการทางการเงิน รวมทั้งหน่วยงานภาครัฐและหน่วยงานภายนอกที่เกี่ยวข้อง

ผู้ให้บริการทางการเงินต้องจัดให้มีกลไกการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับเหตุการณ์ภัยทุจริตดิจิทัลระหว่างผู้ให้บริการทางการเงินและหน่วยงานภายนอกที่เกี่ยวข้องที่สามารถส่งผ่านข้อมูลได้อย่างถูกต้องและรวดเร็ว

1. จัดให้มีกลไกการแลกเปลี่ยนข้อมูลระหว่างผู้ให้บริการทางการเงินกับหน่วยงานกำกับดูแลหรือหน่วยงานที่เกี่ยวข้องที่สามารถส่งผ่านข้อมูลได้อย่างถูกต้องและรวดเร็ว
2. สนับสนุนข้อมูลที่ต้องใช้ในการสืบสวนสอบสวนและติดตามหาผู้กระทำผิดให้แก่พนักงานสอบสวนที่ได้รับมอบหมายเมื่อถูกร้องขออย่างทันกาล

การยกระดับแลกเปลี่ยนข้อมูล	• ระบบ Central Fraud Registry (CFR) ที่สามารถแลกเปลี่ยนข้อมูลสำคัญได้อย่างถูกต้อง ครบถ้วนและมีกลไกที่ช่วยให้ดำเนินการได้ทันที (real time) โดยตัวอย่างข้อมูลสำคัญ ได้แก่ ข้อมูลบัญชีม้าทั้งการแจ้งใหม่และการปลดบัญชี การติดตามเส้นทางเงิน การระงับบัญชี รวมถึงข้อมูลที่จำเป็นต้องใช้ในการประเมินประสิทธิผลและความเหมาะสมของนโยบายทางการ **(ดำเนินการให้แล้วเสร็จภายใน ก.ย. 68)**

4 การสร้างความตระหนักรู้ถึงภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงิน

ผู้ให้บริการทางการเงินมีหน้าที่ในการสร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัลให้แก่ลูกค้าและประชาชน เพื่อป้องกันและลดโอกาสเกิดความเสียหาย

1. สร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัลในลักษณะเชิงรุกอย่างเป็นวงกว้างและสม่ำเสมอ ด้วยวิธีที่เกิดผลอย่างเป็นรูปธรรมในทางปฏิบัติผ่านช่องทางที่ลูกค้าสามารถเข้าถึงได้ง่าย อย่างน้อยเดือนละ 1 ครั้ง เช่น การแจ้งเตือนผ่านแอปพลิเคชันที่ติดตั้งบนอุปกรณ์เคลื่อนที่ การจัดทำสื่อ infographic บนสื่อทางสังคม

2. จัดให้มีการประเมินความตระหนักรู้ต่อภัยทุจริต (awareness test) เมื่อลูกค้าเริ่มต้นใช้บริการ mobile banking และบริการเงินอิเล็กทรอนิกส์ที่โอนเงินได้ ครั้งแรก และประเมินอย่างต่อเนื่องทุก ๆ 6 เดือน เป็นขั้นต่ำ

5 การรายงานข้อมูลต่อธนาคารแห่งประเทศไทย

การรายงานข้อมูล	• ผู้ให้บริการทางการเงินต้องจัดทำและจัดส่งแบบรายงานในรูปแบบและตามระยะเวลาที่ ธปท. กำหนด รวมถึงจัดทำและจัดส่งรายงานและข้อมูลอื่นเพิ่มเติมเป็นรายกรณีตามที่ ธปท. ร้องขอ

6 การเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษ

การเปิดเผยข้อมูล	• กรณีที่ผู้ให้บริการทางการเงินถูกเปรียบเทียบปรับหรือถูกกล่าวโทษอันเนื่องมาจากการปฏิบัติฝ่าฝืนหรือไม่ปฏิบัติตามประกาศฉบับนี้ ให้ผู้ให้บริการทางการเงินเปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษดังกล่าว • ธปท. ขอสงวนสิทธิในการไม่ให้ผู้ให้บริการทางการเงินเปิดเผยข้อมูลการถูกดำเนินการทางกฎหมายตามที่ระบุข้างต้น หากเห็นว่าอาจกระทบกับความปลอดภัยหรือความผาสุกของประชาชน รวมถึงประสิทธิผลของการบริหารจัดการภัยทุจริตดิจิทัล

วันเริ่มต้นบังคับใช้ของหลักเกณฑ์ : 1 เม.ย. 68

ช่องทางการเปิดรับฟังความคิดเห็น

(ร่าง) หลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management)
ช่วงเวลาในการเปิดรับฟังความคิดเห็น 3 – 18 มีนาคม 2568

เอกสารประกอบการรับฟังความคิดเห็น

ช่องทางการรับฟังความคิดเห็นและข้อเสนอแนะ

ติดต่อขอข้อมูลเพิ่มเติม งานจัดการภัยทุจริตทางการเงิน อีเมล **antifraud-policy@bot.or.th**

การจัดทำ SAQ

วัตถุประสงค์	• เพื่อประเมินความพร้อมการปฏิบัติตามหลักเกณฑ์การบริหารจัดการภัยทุจริตดิจิทัล (Digital Fraud Management) ที่คาดว่าจะมีผลบังคับใช้ตั้งแต่วันที่ 1 เม.ย. 2568 • เพื่อนำไปปรับปรุงหลักเกณฑ์ฯ ให้มีความเหมาะสมและไม่เป็นภาระต่อการพัฒนาระบบงานของ สง. มากเกินไป
ขอบเขตการประเมิน	• ครอบคลุมแนวนโยบาย หนังสือเวียน และมาตรการที่เกี่ยวข้องกับ digital fraud ที่ ธปท. ได้สื่อสาร public* • ธพ. / SFIs ที่รับฝากเงิน / ผู้ให้บริการบัตร / ผู้ประกอบธุรกิจ E-money ที่ให้บริการโอนเงินได้
แนวทางการตอบ	• ประเมินตนเองเบื้องต้นว่าผู้ให้บริการได้ทำแล้ว / ทำบางส่วน / ยังไม่ได้ทำ พร้อมอธิบายรายละเอียดเพิ่มเติม เพื่อ ธปท. สามารถนำข้อมูลไปใช้ปรับปรุงหลักเกณฑ์ฯ ต่อไปได้ • จัดทำ SAQ 2 ชุด คือ (1) SAQ สำหรับ ธพ./ SFIs ที่รับฝากเงิน (2) ผู้ให้บริการบัตรและผู้ประกอบธุรกิจ E-money ที่โอนเงินได้ (กรณี ธพ./SFIs ที่ให้บริการบัตร&e-money จัดทำ 2 ชุด) • ส่งเอกสารอ้างอิงที่ สง. มีอยู่แล้ว ไม่ต้องจัดทำเพิ่มเติม
กำหนดส่ง	• หน่วยงาน compliance จัดทำ และอนุมัติ SAQ โดย Head of Compliance • ส่ง SAQ กลับ ธปท. ภายใน 18 มี.ค. 68 (สามารถส่งเอกสารอ้างอิงตามหลังได้ภายใน 31 มี.ค.)

*แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ลงวันที่ 29 มี.ค. 66 และหนังสือที่ ธปท.ฝตท. (01) ว. 384/2567 เรื่อง การเพิ่มความเข้มงวดในการจัดการบัญชีเงินฝาก หรือบัญชีเงินอิเล็กทรอนิกส์ในกรณีลูกค้ามีความเสี่ยงสูงหรือใช้บัญชีที่มีลักษณะหรือพฤติกรรมผิดปกติ ลงวันที่ 31 พ.ค. 67 และมาตรการจัดการบัญชีม้าที่ ธปท. ได้สื่อสารเมื่อวันที่ 30 ม.ค. 68

ประเด็นสอบถามใน SAQ

หลักเกณฑ์	หัวข้อสำคัญ	ประเด็นสอบถามใน SAQ
1. ด้านธรรมาภิบาล	• บทบาทของคณะกรรมการและผู้บริหารระดับสูง • การกำหนดนโยบาย และประเมินผล/ติดตามผล	• บทบาทของคณะกรรมการและผู้บริหารระดับสูง • การกำหนดนโยบาย และประเมินผล/ติดตามผล
2. การบริหารจัดการภัยทุจริตทางการเงิน	การพิสูจน์ตัวตนและรู้จักลูกค้า (KYC/CDD/EDD)	• การจัดระดับความเสี่ยงบัญชีม้าเข้มข้น
	การประเมินและติดตามความเสี่ยง (Monitoring)	• การมีระบบตรวจจับ near real-time / 24x7 • การกำหนดเงื่อนไขการตรวจจับ
	การบริหารจัดการเพื่อป้องกันความเสียหาย	• การกำหนดเพดานวงเงินถอน/โอนเงิน • การมีผลิตภัณฑ์/บริการเสริมเพิ่มความปลอดภัยในการใช้ mobile banking
	การบริหารจัดการเพื่อจำกัดความเสียหาย	• การระงับเงินเข้า-ออกบัญชีม้า • การป้องกันการเปิดบัญชีม้าใหม่
	การแก้ไขสถานการณ์และการดูแลลูกค้า	• การมี hotline 24 ชม. แยกจากช่องทางปกติ • การมีกระบวนการแก้ปัญหา เยียวยาผู้เสียหาย
3. การแลกเปลี่ยนข้อมูล		-
4. ส่งเสริมความรู้ทางการเงิน		-

ตัวอย่าง SAQ

ลำดับ	ประเด็นคำถาม	คำชี้แจงเพิ่มเติม	เอกสารอ้างอิง*
การป้องกันและจำกัดความเสียหายให้แก่ลูกค้า			
7	ผู้ให้บริการมีการกำหนดเพดานวงเงินถอนหรือโอนเงินในช่องทางการทำธุรกรรมต่าง ๆ ให้เหมาะสมตามความระดับเสี่ยงของกลุ่มผู้ใช้บริการแต่ละประเภท ☐ กำหนดแล้ว ☐ ยังไม่กำหนด	*- โปรดอธิบายรายละเอียดการกำหนดเพดานวงเงินการทำธุรกรรมแต่ละกลุ่ม เช่น เงื่อนไขการกำหนดเพดานวงเงินการทำธุรกรรมต่อรายการ/ต่อวัน เงื่อนไขและวิธีการขอปรับเพิ่ม/ลดวงเงินของแต่ละกลุ่ม รวมทั้งจำนวนบัญชีแต่ละกลุ่ม* *- กรณียังไม่กำหนด ขอทราบแนวทางการดำเนินการ และระยะเวลาดำเนินการให้แล้วเสร็จ*	
8	ผู้ให้บริการจัดให้มีผลิตภัณฑ์/บริการ mobile banking ที่ช่วยเพิ่มความปลอดภัยในการใช้บริการ โดยผู้ใช้บริการสามารถบริหารจัดการความเสี่ยงในการทำธุรกรรมได้ด้วยตนเอง เช่น - มีทางเลือกให้ลูกค้าสามารถล็อคเงินในบัญชีไม่ให้ทำธุรกรรมผ่านช่องทางอิเล็กทรอนิกส์ และปลดล็อคได้ยากขึ้น (Money lock) - ปรับลดค่าวงเงินในการสแกนใบหน้าการทำธุรกรรมใน mobile banking ☐ มีบริการ ☐ ยังไม่มีบริการ	*- โปรดอธิบายรายละเอียด และเงื่อนไขการใช้ผลิตภัณฑ์หรือบริการ รวมถึงผลิตภัณฑ์/บริการอื่น ๆ นอกเหนือจากที่ ธปท. กำหนด* *- กรณียังไม่ได้จัดทำ ขอทราบเหตุผล ข้อจำกัด และระยะเวลาดำเนินการให้แล้วเสร็จ*	*เอกสารแสดงผลิตภัณฑ์/บริการดังกล่าว เช่น mobile app. screen เอกสารสมัครการใช้บริการ*

การตรวจ thematic exam

วัตถุประสงค์	• เพื่อประเมินการบริหารจัดการภัยทุจริตดิจิทัลจากการทำธุรกรรมทางการเงินของ สง. ให้เป็นไปตามหลักเกณฑ์ Digital Fraud Management โดยหน่วยงานกำกับของ สง. มีส่วนร่วมในการประเมินด้วย
ขอบเขตการตรวจสอบ	• ให้หน่วยงาน internal audit ตรวจสอบการปฏิบัติตามหลักเกณฑ์ Digital Fraud Management โดยใช้ผลประเมินและเอกสารอ้างอิงจาก SAQ ประกอบการตรวจสอบเพิ่มเติมด้วย • ธพ. / SFIs ที่รับฝากเงิน / ผู้ประกอบธุรกิจ E-money ที่ให้บริการโอนเงินได้
กำหนดส่ง	• หน่วยงาน internal audit จัดทำรายงานตรวจสอบ และขอความเห็นชอบจาก CEO • ส่งรายงานตรวจสอบกลับ ธปท. ภายในสิ้นเดือน ก.ค. 68 (เริ่มตรวจสอบหลัง 1 เม.ย. 68)

Timeline การบังคับใช้

4 มี.ค. 68
- ออก Consultation paper และ hearing ผู้ที่เกี่ยวข้อง
- ออก SAQ high priority

18 มี.ค. 68
- ปิดรับฟังความคิดเห็น
- ผู้ให้บริการส่ง SAQ กลับมายัง ธปท.

31 มี.ค. 68
- ผู้ให้บริการส่งเอกสารอ้างอิงใน SAQ กลับมายัง ธปท.

1 เม.ย. 68 ออกหลักเกณฑ์
- ประกาศ Digital Fraud Risk Management
- หนังสือเวียนมาตรฐานขั้นต่ำการจัดการบัญชีม้า
- หนังสือเวียนยกระดับ CDD/EDD

30 มิ.ย. ออกหลักเกณฑ์
- ประกาศ KYC/CDD/EDD (end-to-end)
- ยกระดับแนวนโยบายเป็นประกาศ KYM

31 ก.ค. 68
- ผู้ให้บริการส่งรายงานตรวจสอบกลับมายัง ธปท.

ไตรมาส 3 : thematic exam ด้าน digital fraud