ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

- ร่าง -

แนวนโยบายการบริหารจัดการภัยทุจริต จากการทำธุรกรรมทางการเงิน

23 พฤศจิกายน 2565

1. เหตุผลความจำเป็น
2. หลักการและขอบเขตการบังคับใช้
3. แนวนโยบาย
4. Q&A

โลกดิจิทัลภัยทุจริตเพิ่มขึ้นต่อเนื่อง หลากหลายรูปแบบมากขึ้น ส่งผลกระทบต่อประชาชนในวงกว้างอย่างรวดเร็ว

รูปแบบภัยทุจริตหลากหลายและเกิดขึ้นได้ในทุกขั้นตอน

- ATM card skimming
- Social engineering
- ปลอมสลิปโอนเงิน

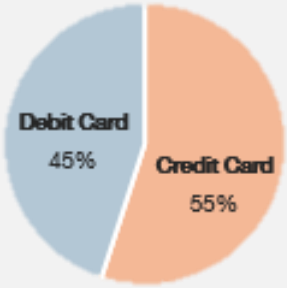
- สวมรอยเปิดบัญชี/ บัญชีม้า
- Account takeover

106,000 บัญชี
1,300 รายการ 96 ล้านบาท

- ข้อมูลรั่วไหล
- Bin attack

เมื่อ ต.ค. 64 บัตรจำนวน 10,700 ใบ
ความเสียหาย 130 ล้านบาท

800,000 รายการ 1,200 ล้านบาท



หมายเหตุ: ข้อมูลสถิติจากภัยทุจริตผ่านช่องทางต่าง ๆ ในปี 2564 ของ สง. 9 แห่ง

หลักการ

01

ป้องกันช่องโหว่ในการกระทำทุจริตหรือภัยคุกคามทางการเงินอย่างเท่าทัน

02

Risk UX/UI

สร้างสมดุลระหว่าง
การบริหารจัดการความเสี่ยงที่รัดกุมเพียงพอและ
การส่งเสริมธุรกรรมการเงินทางอิเล็กทรอนิกส์

03

คุ้มครองผู้ใช้บริการ
อย่างเหมาะสมเป็นธรรม

Intended Outcome

1. การยกระดับ Fraud Risk เป็นความเสี่ยงระดับองค์กร
2. การบริหารจัดการภัยทุจริตเป็นไปอย่างต่อเนื่องและทันการณ์
3. ลูกค้าได้รับการดูแลผลกระทบที่เกิดขึ้นอย่างเหมาะสมและทันกาล
4. พนักงานและผู้ใช้บริการได้รับการสร้างความตระหนักในเชิงรุกและต่อเนื่อง
5. มีกลไกความร่วมมือและการแลกเปลี่ยนข้อมูลอย่างมีบูรณาการ

ขอบเขตการบังคับใช้

สถาบันการเงิน	สถาบันการเงินเฉพาะกิจ	ผู้ประกอบธุรกิจระบบการชำระเงินและบริการการชำระเงินภายใต้การกำกับ

“การทำธุรกรรมทางการเงิน”

ธุรกรรมทางการเงินที่ผู้ให้บริการทางการเงินให้บริการ ***ได้แก่ การเปิดบัญชี การสมัครใช้บริการ การฝากเงิน การถอนเงิน การโอนเงิน และการชำระค่าสินค้าและบริการ เป็นต้น*** *โดยผ่านช่องทางการให้บริการครอบคลุม* ***สาขาทั่วไป สาขาอิเล็กทรอนิกส์ ช่องทางดิจิทัล (digital channels) หรือช่องทางให้บริการอื่น****ที่ธนาคารแห่งประเทศไทยอนุญาตเพิ่มเติมทั้งที่เป็นการทำธุรกรรมทางการเงินผ่านบัตรหรือผ่านสื่ออื่น เช่น QR code*

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

- ร่าง
-

แนวนโยบายการบริหารจัดการภัยทุจริต จากการทำธุรกรรมทางการเงิน

- ร่าง -

แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน

1. ด้านธรรมาภิบาล

2. ด้านบริหารจัดการภัยทุจริต

- การป้องกันภัย (Protection)
- การตรวจจับ (Detection)
- การตอบสนองและการรับมือ (Response)
- ความร่วมมือ (Collaboration)

เอกสารแนบ 1 : การบริหารจัดการภัยทุจริตจากการทำธุรกรรมการชำระเงินผ่านบัตร
เอกสารแนบ 2 : การบริหารจัดการปัญหาการทุจริตและหลอกลวงผ่านการใช้บัญชีเงินฝากหรือบัญชีอิเล็กทรอนิกส์

- ร่าง -

“ภัยทุจริต” เป็นความเสี่ยงสำคัญขององค์กร

- มี**คณะกรรมการและผู้บริหารระดับสูง**ทำหน้าที่กำหนดนโยบายและการกำกับดูแลอย่างชัดเจน
- มี**นโยบาย**ในการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน
- **ประเมิน วัดผล และติดตามประสิทธิภาพและประสิทธิผล**ของการจัดการภัยทุจริตโดยรายงานผลประเมินอย่างต่อเนื่อง
- **สร้างความตระหนักรู้**อย่างบูรณาการทั่วทั้งองค์กร รวมทั้ง **เตือนภัยผู้ใช้บริการ**ไม่ให้ตกเป็นเหยื่อของมิจฉาชีพแก่อย่างต่อเนื่องและทันการณ์

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

- ร่าง -

การป้องกันภัย (Protection)

การตรวจจับ (Detection)

การตอบสนองและการรับมือ (Response)

ความร่วมมือ (Collaboration)

“ป้องกันภัยทุจริต” by design

- *นำปัจจัยด้านการป้องกันภัยทุจริตมาใช้ในการพิจารณา**ตั้งแต่เริ่มต้นการออกแบบ พัฒนา หรือปรับปรุงผลิตภัณฑ์***
- ***มีมาตรการการป้องกันภัยทุจริต ตั้งแต่การสมัคร/เปิดใช้บริการ การทำธุรกรรม จนถึงการปิด/ยกเลิก** ครอบคลุม*
    - *การพิสูจน์และยืนยันตัวตนในการทำธุรกรรมตามระดับความเสี่ยง*
    - *การรักษาความปลอดภัยของข้อมูล*
    - *มีระบบหรือช่องทางรองรับให้ผู้ใช้บริการจัดการความเสี่ยงในการทำธุรกรรมได้ด้วยตนเอง และแจ้งเตือนการทำธุรกรรมผ่านช่องทางต่าง ๆ*
- ***ทบทวนและปรับปรุง** การป้องกันภัยทุจริตอย่างสม่ำเสมอ*

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

- ร่าง -

การป้องกันภัย (Protection)

การตรวจจับ (Detection)

การตอบสนองและการรับมือ (Response)

ความร่วมมือ (Collaboration)

“ตรวจจับ” ยับยั้งและจำกัดความเสียหายได้อย่างรวดเร็ว

- มี**บุคลากร กระบวนการ และระบบ**ในการตรวจจับและติดตามความผิดปกติ (fraud monitoring)
- กำหนดเงื่อนไขในการตรวจจับให้**ครอบคลุมรูปแบบภัยทุจริต**ในแต่ละช่องทางการให้บริการ และสามารถแจ้งเตือน**แบบ early warning** รวมทั้ง ปรับปรุงประสิทธิภาพการตรวจจับให้ลักษณะเป็น**เชิงรุก**
- มี**ช่องทางในการรับแจ้งเบาะแสหรือการรายงาน**กรณีมีเหตุการณ์ต้องสงสัย ทั้งจากภายในและภายนอกองค์กร
- **ทบทวนและปรับปรุง** การตรวจจับภัยทุจริตอย่างสม่ำเสมอ รวมทั้ง อาจพิจารณานำเทคโนโลยีใหม่ ๆ เช่น data analytics , Artificial Intelligence มาใช้เพิ่มประสิทธิภาพ

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

- ร่าง -

การป้องกันภัย (Protection)

การตรวจจับ (Detection)

การตอบสนองและการรับมือ (Response)

ความร่วมมือ (Collaboration)

“ตอบสนองและรับมือ” ช่วยเหลือและเยียวยาได้อย่างเหมาะสมทันการณ์

- ***กำหนดกระบวนการ****ตอบสนองและรับมือต่อเหตุการณ์ภัยทุจริต รวมทั้ง* ***ซักซ้อม****กับให้ฝ่ายงานที่เกี่ยวข้อง*
- ***กำหนด Service Level Agreement*** *ในการดูแลผู้ใช้บริการที่ได้รับผลกระทบจากความเสียหายที่เกิดขึ้นให้ชัดเจน*
- ***กำหนดกระบวนการในการรายงาน****เหตุการณ์ทุจริตแก่คณะกรรมการและผู้บริหารระดับสูงที่มีหน้าที่รับผิดชอบ รวมทั้ง ต้องรายงานเหตุการณ์ทุจริตที่ก่อให้เกิดความเสียหายกับผู้ใช้บริการในวงกว้างหรือส่งผลกระทบ*
  ต่อชื่อเสียงของผู้ให้บริการทางการเงิน ***ให้ ธปท. ทราบโดยเร็ว***

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

- ร่าง -

การป้องกันภัย (Protection)

การตรวจจับ (Detection)

การตอบสนองและการรับมือ (Response)

ความร่วมมือ (Collaboration)

“ร่วมมือ” ลดภัยทุจริตอย่างยั่งยืน

- ***สร้างกลไกความร่วมมือและแลกเปลี่ยนข้อมูล*** *โดยกำหนดแนวทาง กระบวนการ และช่องทางการสื่อสารประสานงานระหว่างผู้ให้บริการกับหน่วยงานกำกับดูแล หรือหน่วยงานที่เกี่ยวข้อง ทั้งนี้ การแลกเปลี่ยนข้อมูล*
  อาจพิจารณาจัดให้มีระบบการแลกเปลี่ยนข้อมูลการทุจริต และพัฒนาระบบฐานข้อมูลกลางด้านทุจริตในระยะต่อไป
- ***ร่วมกันสร้างความรู้และความตระหนักรู้****แก่ประชาชนในลักษณะเชิงรุกและมีบูรณาการ*
- *กรณีเกิดเหตุการณ์ทุจริตจากพร้อมกันในหลายผู้ให้บริการ และส่งผลกระทบในวงกว้างต่อความเชื่อมั่นของระบบการเงิน* ***สมาคมธนาคารไทยและสมาคมอื่นที่เกี่ยวข้อง ควรร่วมกันกำหนดแนวทางช่วยเหลือ***

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

สำหรับการทำธุรกรรมการชำระเงินผ่านบัตร และบริการที่เกี่ยวข้องกับการเปิดบัญชีเงินฝากหรือเปิดใช้บริการเงินอิเล็กทรอนิกส์

ให้ปฏิบัติเพิ่มเติมตามข้อกำหนดด้านบริหารจัดการภัยทุจริตในเอกสารแนบด้วย

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

เอกสารแนบ 1: การบริหารจัดการภัยทุจริตจากการทำธุรกรรมการชำระเงินผ่านบัตร

- ร่าง -

การป้องกันภัย

- ***ยืนยันตัวตนผู้ถือบัตร*** *ให้สอดคล้องกับระดับความเสี่ยงของธุรกรรม*
- ***มีมาตรการ Data Security*** *สอดคล้องตามมาตรฐานสากล เช่น PCIDSS รวมทั้ง* ***นำเทคโนโลยีหรือวิธีการใหม่ ๆ มาใช้ยกระดับ*** *เช่น การใช้ Tokenization*
- *มีระบบรองรับให้ผู้ถือบัตรสามารถกำหนดการตั้งค่าได้****ด้วยตนเอง***

การตรวจจับ

- *มีระบบ Fraud monitoring ตรวจจับ****แบบ near real-time และต่อเนื่อง 24x7***
- ***กำหนดเงื่อนไขขั้นต่ำ****แบบ early warning เพื่อให้ครอบคลุมรูปแบบภัยทุจริต ที่เกิดขึ้น เช่น BIN Attack*

การตอบสนองและการรับมือ

- ***ติดต่อกลับผู้ถือบัตรภายใน 1 ชม.*** *หลังจากได้รับแจ้งเหตุ และ****แจ้งความคืบหน้าในเบื้องต้นให้ผู้ถือบัตรทราบภายใน 24 ชม.*** *นับจากได้รับแจ้งจากผู้ถือบัตร*
- *การเยียวยาเมื่อผู้ถือบัตรได้รับความเสียหาย*

  (1) ***บัตรเดบิต*** *ให้คืนเงินให้ผู้ถือบัตร****ภายใน 5 วันทำการ*** *หลังจากได้รับแจ้ง*

  (2) ***บัตรเครดิต*** *ให้ยกเลิกรายการดังกล่าว*

ความร่วมมือ

ให้ผู้ประกอบธุรกิจระบบเครือข่ายบัตร *จัดให้มีมาตรการส่งเสริมและสนับสนุน ให้สมาชิกเครือข่ายบัตรของตนอย่างชัดเจนและต่อเนื่อง*

- *กำหนด****แผนงานเพื่อให้สมาชิกเครือข่ายบัตรยกระดับ****ความมั่นคงปลอดภัย และระบบการบริหารจัดการความเสี่ยงจากการทำธุรกรรมผ่านบัตร*
- ***มีระบบและกลไกการประสานงานร่วมกับสมาชิกเครือข่ายบัตรในการช่วยเหลือให้สมาชิก*** *โดยสนับสนุนข้อมูลที่เป็นประโยชน์แก่สมาชิกเพื่อนำไปพัฒนาระบบการป้องกันและตรวจจับภัยให้มีประสิทธิภาพมากยิ่งขึ้น*

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

เอกสารแนบ 2: การบริหารจัดการปัญหาการทุจริตและหลอกลวงผ่านการใช้บัญชีเงินฝากหรือบัญชีอิเล็กทรอนิกส์

- ร่าง -

การป้องกันภัย

- การเปิดบัญชีแบบ non-face-to-face ในครั้งต่อไปให้กับลูกค้าปัจจุบัน ต้องมีวิธีการยืนยันตัวตนลูกค้าที่รัดกุมโดยใช้ **biometric comparison และ liveness detection เป็นขั้นต่ำ**
- ให้ชื่อเจ้าของบัญชี**สอดคล้องตรงกัน**กับชื่อเจ้าของเลขหมายโทรศัพท์
- กำหนดให้ลูกค้า 1 รายสามารถเปิดใช้บัญชี mobile banking หรือบัญชีกระเป๋า e-Wallet ของผู้ให้บริการแต่ละรายได้เพียง 1 บัญชีต่อ 1 ผลิตภัณฑ์และจำกัดให้ใช้งานบน 1 อุปกรณ์เท่านั้น
- ลูกค้า**สามารถระงับบัญชีชั่วคราวได้ด้วยตนเอง**บน mobile banking หรือกระเป๋า e-Wallet
- กำหนดวงเงินสงสดต่อวันตามความระดับเสี่ยง กรณี **กลุ่มเยาวชนอายุต่ำกว่า 15 ปี ให้ 50,000 บาทต่อวัน**

การตอบสนองและการรับมือ

- ปฏิบัติตามกฎกระทรวง ประกาศ หรือหลักเกณฑ์ตามกฎหมาย ปปง. อย่างเคร่งครัด
- งดเว้นแนบลิงก์ผ่านช่องทาง SMS อีเมล และ โซเชียลมีเดีย **ในการขอข้อมูลสำคัญ**
- **ดำเนินการ ระงับ อายัด จำกัดวงเงิน โดยทันที** ตามที่ระบุในหนังสือจากพนักงานสอบสวน
- สื่อสารให้ทันกับสถานการณ์ ทั้งกับหน่วยงานภายในและภายนอก

การตรวจจับ

- กำหนดเงื่อนไขการตรวจจับและติดตามธุรกรรม**ที่เข้าข่าย บัญชีม้า เป็นขั้นต่ำ**
- กรณีตรวจพบบัญชีม้าหรือการหลอกลวงจำนวนมาก อาจพิจารณากำหนดเงื่อนไขเพิ่มเติม

ความร่วมมือ

- **สนับสนุนข้อมูลให้แก่พนักงานสอบสวน**ที่ได้รับมอบหมายจากระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติโดยเร็ว โดยจัดเตรียมข้อมูลอย่างน้อย (1) IP address (2) ข้อมูลการทำธุรกรรม (3) หมายเลขโทรศัพท์
- **สนับสนุนหน่วยงานของรัฐ**ที่เกี่ยวข้องในการสื่อสารแก่ประชาชนผ่านช่องทาง ที่เข้าถึงได้ง่าย โดยแจ้งเตือนภัยทุจริตและหลอกลวงออนไลน์ต่าง ๆ บนระบบ mobile banking หรือกระเป๋า e-Wallet

ธนาคารแห่งประเทศไทย
BANK OF THAILAND