ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ยกระดับการกำกับและการปฏิบัติตามกฎหมายว่าด้วยระบบการชำระเงิน

10 มีนาคม 2569

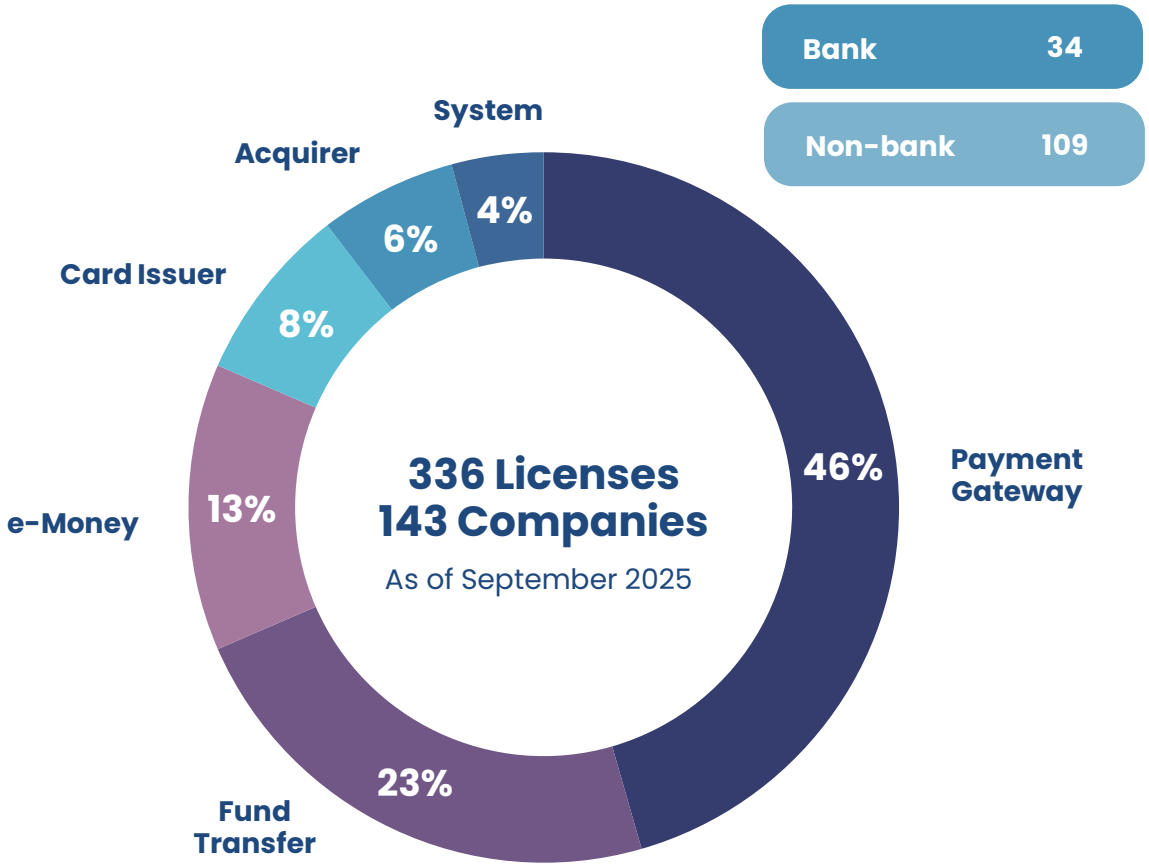
ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Payment Market Overview (1)

Increasing Competition in Online Payment Gateway

Capturing Opportunities in Cross-border Payments

Fraud Mitigation Mechanism



ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Regulation Update

Intended outcome :

Trustworthiness | **Efficiency** | **Inclusion**

Enhanced PromptPay

ยกระดับการกำกับดูแลระบบการชำระเงินรายย่อยที่มีนัยสำคัญต่อระบบการเงิน (Systemically Important Retail Payment System: SIRPS)

Enhanced Fraud Regulations

- ประกาศ Mobile Banking Security
- ประกาศ Shared Responsibility (Payment)
- ประกาศ Digital Fraud Management (DFM)
- ประกาศ Card Fraud Management (CFM) *
- ประกาศ Merchant Fraud Management (MFM) *

ออกประกาศแล้ว
อยู่ระหว่างดำเนินการ

* ยกระดับการกำกับดูแลจากแนวปฏิบัติ

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ภาพรวมหลักเกณฑ์ที่เกี่ยวข้องกับระบบ SIRPS

1. หลักเกณฑ์การประเมินระบบ SIRPS

1.1 กำหนดปัจจัยที่ใช้ประเมิน SIRPS

1.2 กำหนดระบบที่มีเป็น SIRPS (ระบบพร้อมเพย์)

2. หลักเกณฑ์การประกอบธุรกิจระบบที่จัดเป็น SIRPS

ยกระดับการปฏิบัติงานและการบริหาร

จัดการความเสี่ยง ในประเด็นที่สำคัญเพิ่มเติมจากระบบการชำระเงินรายย่อย

- ด้านธรรมาภิบาล
- ด้านการบริหารความเสี่ยงและความมั่นคงปลอดภัย
- ด้านการคุ้มครองและส่งเสริมการแข่งขันของผู้ใช้บริการของระบบ (access & fee)

3. หลักเกณฑ์การกำกับดูแลการให้บริการผ่านระบบ SIRPS

เพื่อบริหารจัดการระหว่างผู้ใช้บริการของระบบ ให้สามารถใช้ประโยชน์ร่วมกัน

อย่างมีประสิทธิภาพ เป็นธรรม

สามารถ

ดูแลความมั่นคงปลอดภัยของระบบ และดูแลลูกค้าอย่างเหมาะสม

- ข้อตกลงทางธุรกิจ (Scheme Rule)
- Payment Service Fee ที่โปร่งใส เป็นธรรม เสมอภาค ไม่ปิดกั้นการเข้าถึงระบบ

ภาพรวมหลักเกณฑ์เกี่ยวกับการจัดการภัยทุจริตสำหรับผู้ประกอบธุรกิจการชำระเงิน

	1 Shared Responsibility (Payment)	2 Mobile Banking Security (Payment)	3 Digital Fraud Management (DFM)	4 Card Fraud Management (CFM)	5 Merchant Fraud Management (MFM)
อำนาจกฎหมาย	พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และ 2568 (ฉบับที่ 1 และ 2)	พ.ร.บ.ระบบการชำระเงิน พ.ศ. 2560	พ.ร.บ.สถาบันการเงิน พ.ศ. 2551 พ.ร.บ.ระบบการชำระเงิน พ.ศ. 2560	พ.ร.บ.ระบบการชำระเงิน พ.ศ. 2560	พ.ร.บ.ระบบการชำระเงิน พ.ศ. 2560
การบังคับใช้	11 ธันวาคม 2568	มีผลบังคับใช้หลังจาก 30 วัน / 90 วัน นับแต่วันที่ 8 ส.ค. 68 (แล้วแต่เรื่อง)	4 ธันวาคม 2568 เว้นแต่ข้อ 5.3.1 ให้บังคับใช้เมื่อพ้นกำหนด 90 วันนับแต่วัดจากประกาศฯ	อยู่ระหว่างดำเนินการ	อยู่ระหว่างดำเนินการ
หลักการ	- เป็นมาตรฐานและมาตรการในการป้องกันอาชญากรรมทางเทคโนโลยี เพื่อช่วยลดความเสียหายต่อประชาชน รักษาความเชื่อมั่นในระบบ สง. และระบบการชำระเงิน - กรณีเกิดความเสียหายที่เกี่ยวข้องโดยตรงกับการที่ ผปก. ไม่ปฏิบัติตามหลักเกณฑ์นี้ ผปก. ต้องมีส่วนร่วมรับผิดชอบตามสัดส่วนแห่งพฤติการณ์	ยกระดับการให้บริการ e-Money mobile application ให้มีมาตรฐานขั้นต่ำที่จำเป็น ประกอบด้วยมาตรการ 2 ส่วน (1) การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (unauthorized payment fraud) (2) การรักษาความมั่นคงปลอดภัยของบริการ e-Money mobile application	เป็นแนวทางในการบริหารจัดการภัยทุจริตดิจิทัล แบบ end-to-end ตั้งแต่การป้องกัน ติดตามและตรวจจับ จัดการและแก้ไข รวมทั้งดูแลลูกค้าที่ได้รับผลกระทบ เพื่อให้การบริหารจัดการภัยทุจริตดิจิทัลเป็นไปอย่างมีประสิทธิผล สอดรับกับสภาพแวดล้อม ป้องกันและลดความเสียหาย รักษาความเชื่อมั่นในระบบ สง. และระบบการชำระเงิน	ยกระดับความปลอดภัยในการใช้งานบัตร โดยต้องมีการบริหารจัดการภัยทุจริต แบบ end-to-end ตั้งแต่การป้องกัน ติดตามและตรวจจับ จัดการและแก้ไขเมื่อเกิดเหตุภัยทุจริต รวมทั้งดูแลลูกค้าที่ได้รับผลกระทบ	ยกระดับการบริหารจัดการความเสี่ยงร้านค้าให้ได้มาตรฐานและสามารถป้องกันภัยทุจริตได้อย่างมีประสิทธิผล ตั้งแต่การกำหนดนโยบายและมาตรการบริหารความเสี่ยง การประเมินและจัดระดับความเสี่ยงร้านค้า การรู้จักร้านค้า และการบริหารจัดการความเสี่ยงร้านค้า รวมถึงการดูแลร้านค้าเมื่อเกิดเหตุภัยทุจริต

ขอบเขตการบังคับใช้

บัญชีเงินฝาก	☑ (ตามประกาศ Shared Resp. สำหรับ สง.)	☑ (ตามประกาศ MBS สำหรับ สง.)	☑		
[1] e-Money	☑ (เฉพาะ e-Money รับอนุญาต)	☑ (e-Money รับอนุญาตซึ่งสามารถโอนเงินไปยังบัญชีของบุคคลอื่นที่มีอยู่กับผู้ให้บริการทางการเงินอื่น)	☑	☑ (e-Money รับอนุญาต ซึ่งให้บริการ e-Money ในรูปแบบบัตรที่ใช้บริการระบบเครือข่ายบัตร)	☑
[2] โอนเงิน	☑		☑		
[3] Card Issuer (Credit/Debit/ATM)	☑ (เฉพาะ Credit และ Debit)			☑	
[4] Acquirer	☑			☑	☑
[5] Payment Facilitator	☑			☑	☑
[6] รับชำระเงินแทน	☑				☑
[7] ระบบโอนเงินรายย่อย			☑		
[8] ระบบเครือข่ายบัตร				☑	

1 Shared Responsibility : e-Payment

หลักการ แก้ปัญหาบัญชีม้าได้ตรงจุด สอดคล้องกับบริบทไทย วิธีปฏิบัติชัดเจน

ขอบเขต e-Money ที่ใช้วงกว้าง (ต้องได้รับอนุญาต) / Card Issuing (บัตรเครดิต) / กลุ่มรับชำระเงินให้ร้านค้า (Acquirer/ Payment Facilitator/ Bill Payment) และโอนเงิน

		e-Money อนุญาต	Issuer (บัตรเครดิต)	รับชำระให้ร้านค้า	โอนเงิน
การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ	• ห้ามส่ง SMS แนบลิงก์ที่เป็นเหตุให้เกิดความเสียหาย • จำกัดให้ผู้ใช้บริการ e-Money ผ่าน Mobile Application ใช้งานได้บน 1 device เท่านั้น • Face scan โอนเงิน • ป้องกันการแก้ไข App • ไม่ให้ใช้งานบนอุปกรณ์ที่มี App เสี่ยง	✓1/			
การทำ KYC/CDD ลูกค้าและร้านค้า	• มีกระบวนการทำความรู้จักลูกค้าทั้งในการแสดงตนลูกค้า(Identification) และการพิสูจน์ตัวตนลูกค้า (Verification) ตามหลักเกณฑ์ KYC	✓			✓
	• มีกระบวนการทำความรู้จักเจ้าของร้านค้าหรือผู้มีอำนาจจัดการร้านค้าทั้งบุคคลธรรมดาหรือนิติบุคคล ตามหลักเกณฑ์ ปปง. และ ธปท.	✓		✓	
	• จัดระดับลูกค้า/ร้านค้าที่เป็นม้าเป็นความเสี่ยงสูง และ Take action ตามมาตรการจัดการบัญชีม้า หากไม่สามารถ EDD ได้	✓	✓	✓	✓
การจำกัดความเสียหายและการจัดการบัญชีม้า	• แจ้งเตือนลูกค้าทันที เมื่อเงินออกจากบัญชี e-Money หรือมีธุรกรรมชำระเงินด้วยบัตร โดยไม่มีค่าใช้จ่าย	✓2/	✓		
	• ระงับการทำธุรกรรมและต่อเส้นเงินตามแนวทางที่ ศปอท. กำหนด	✓	✓	✓	✓
	• ระงับการทำธุรกรรมระดับบุคคล (ระงับเงินเข้า / ระงับเงินออก / ปฏิเสธการเปิดบัญชีหรือการทำธุรกรรม ตามลักษณะบริการ)	✓3/	✓		✓
	• ระงับการ settlement เงินเข้าบัญชีที่เจ้าของร้านค้า/ผู้มีอำนาจจัดการร้านค้ามีรายชื่อในฐานข้อมูลบัญชีม้า	✓		✓	
กระบวนการรับแจ้งเหตุ	• มีช่องทางติดต่อเร่งด่วนที่สามารถติดต่อได้ ทั้งในและนอกเวลาทำการ	✓	✓		✓

[1/] เฉพาะกลุ่ม e-Money โอนเงินต่างชื่อต่างสถาบัน

[2/] เฉพาะกลุ่ม e-Money ที่ให้บริการผ่าน mobile application

[3/] กรณีกลุ่มบัตร e-Money ที่ใช้ชำระเงิน ให้ดำเนินการเฉพาะการปฏิเสธการเปิดบัญชีใหม่

2 Mobile Banking Security – ePayment

หลักการ

e-Money มีมาตรฐานการควบคุมขั้นต่ำที่จำเป็นสำหรับการให้บริการ Mobile Banking อย่างปลอดภัย [E2E] เท่าทันความเสี่ยง Cyber และ unauthorized payment fraud ที่มีการปรับเปลี่ยนรูปแบบและมีเทคนิคซับซ้อนขึ้น

ขอบเขต

e-Money ที่มีการให้บริการ Mobile Application ซึ่งสามารถโอนเงินไปยังบัญชีของบุคคลอื่นที่มีอยู่กับผู้ให้บริการทางการเงินอื่น

Target

1. ลูกค้า

มาตรการป้องกันการสวมรอยทำธุรกรรมแทนลูกค้า

สวมรอยเป็นผู้ให้บริการทางการเงิน

- งดแนบ link ผ่าน SMS และ email และงดแนบ link ขอข้อมูลสำคัญผ่าน social media
- มีกระบวนการติดตาม และ takedown แอปปลอมเป็นธนาคาร

สวมรอยเป็นลูกค้า

- Face scan เมื่อโอนเงิน ตั้งแต่ 50,000 บาทต่อครั้ง หรือ 200,000 บาทต่อวัน หรือปรับเพิ่มวงเงินโอนเงินต่อวัน ให้โอนได้ตั้งแต่ 50,000 บาทขึ้นไป
- จำกัดให้ผู้ใช้บริการ e-Money สามารถใช้งานแต่ละ Mobile Application ได้บนอุปกรณ์เคลื่อนที่ 1 อุปกรณ์เท่านั้น

2. Mobile App

มาตรการรักษาความปลอดภัย Mobile Application

Secure Data

- ไม่เก็บข้อมูลสำคัญบนเครื่อง และต้องเข้ารหัสข้อมูล
- แสดงข้อมูลสำคัญเท่าที่จำเป็น
- ใช้ช่องทางสื่อสารที่ปลอดภัย (secure protocol) และยืนยันตัวตนด้วย certificate pinning

Secure Mobile Application

- ขอ permission เฉพาะที่จำเป็น
- ไม่อนุญาตให้ใช้ MB เวอร์ชันเก่าที่มีช่องโหว่
- **ป้องกันการแก้ไขแอป**
- ป้องกัน session hijacking
- ป้องกัน source code รั่วไหล

Secure Device

- **ไม่ให้ใช้งานบนอุปกรณ์ที่ไม่ปลอดภัย เช่น root /jailbreak**
- **ไม่ให้ใช้บนอุปกรณ์ที่ติดตั้งแอปที่มีพฤติกรรมผิดปกติ**
- หลีกเลี่ยงการให้ใช้งานบนอุปกรณ์ที่ Obsolete OS

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

3 Digital Fraud Management (DFM)

การยกระดับแนวนโยบายและหนังสือเวียนที่เกี่ยวข้องกับการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน (ปี 66 และ 67)

Intended Outcome	ผู้ให้บริการทางการเงินมีกระบวนการป้องกัน ติดตามและตรวจจับ จัดการและแก้ไข รวมทั้งดูแลลูกค้าที่ได้รับผลกระทบ

ขอบเขต: [1] ธนาคารพาณิชย์ / SFIs ที่รับฝากเงินจากประชาชน / E-money ที่โอนเงินไปยังบัญชีบุคคลอื่นที่มีอยู่กับผู้ให้บริการอื่นได้ (ทุกข้อ)
[2] บง. บค. ผู้ประกอบธุรกิจ E-payment อื่น และบริษัทลูกในต่างประเทศที่ประกอบธุรกิจ ธพ. หรือ e-money (ปรับใช้ตามความเหมาะสม)

หลักการ Digital Fraud Management
ต้องดำเนินการอย่างเหมาะสมและทันกาล โดยต้องสร้างความสมดุลระหว่างความสะดวก
และความปลอดภัยในการทำธุรกรรมทางการเงิน และคำนึงถึงการคุ้มครองลูกค้าอย่างเป็นธรรม

Governance คณะกรรมการและผู้บริหารระดับสูงให้ความสำคัญกับ Digital Fraud Management

1 ตรวจจับภัยทุจริตดิจิทัล	2 จัดการภัยทุจริตดิจิทัล	3 ดูแลหลังเกิดภัยทุจริตดิจิทัล
การรู้จักลูกค้า (KYC/CDD/EDD) "ประเมินความเสี่ยงของลูกค้า"	**การบริหารจัดการภัยทุจริตดิจิทัล (Action)** "ป้องกัน จำกัด ระงับความเสียหาย"	**การแก้ไขปัญหาและดูแลลูกค้า (Response)** "รับแจ้งเหตุ สื่อสาร ปลดระงับ และเยียวยาลูกค้า ชัดเจน รวดเร็ว เป็นธรรม"
การประเมินและติดตามความเสี่ยง (Monitoring) "ตรวจจับและติดตาม ความผิดปกติ รวมถึงมีกระบวนการติดตามและปรับปรุงสม่ำเสมอ"	**ป้องกันเหยื่อ** "เตือนและหน่วง" **จัดการม้า** "ระงับธุรกรรม"	

Enabler

- **กระบวนการแลกเปลี่ยนข้อมูล** "ระบบ CFR ติดตามเส้นเงิน + สนับสนุนข้อมูลให้ตำรวจได้รวดเร็ว"
- **ส่งเสริมความรู้ทางการเงิน** "ประชาชนไม่ตกเป็นเหยื่อมิจฉาชีพ"

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

กรอบแนวทางขั้นต่ำในการบริหารจัดการภัยทุจริตดิจิทัล

[Minimum expectation ของประกาศ DFM]

Objective

ผู้ให้บริการทางการเงินมีแนวปฏิบัติที่ชัดเจนที่ต้องดำเนินการตามหลักการของประกาศ DFM โดยนำมาตรการ/มาตรฐานอุตสาหกรรมที่ ธปท. เคยสื่อสารให้ผู้ให้บริการทางการเงินทราบแล้ว มากำหนดให้เป็นมาตรฐานหรือยกระดับให้เข้มข้นขึ้น

ขอบเขต: [1] ธนาคารพาณิชย์ / SFIs ที่รับฝากเงินจากประชาชน

[2] ผู้ประกอบธุรกิจ E-money และ ผู้ประกอบธุรกิจบริการโอนเงินด้วยวิธีการทางอิเล็กทรอนิกส์

หลักการ Digital Fraud Management

Governance “กำหนดเป้าหมายและตัวชี้วัดให้ครบถ้วน end-to-end และกำหนดหน้าที่ของหน่วยงานตรวจสอบภายใน”

1 ตรวจจับภัยทุจริตดิจิทัล

การรู้จักลูกค้า (KYC/CDD/EDD)

การประเมินและติดตามความเสี่ยง (Monitoring)

“มีแนวทางนำ data analytics / AI หรือเทคโนโลยีอื่นมาพัฒนาระบบตรวจจับทั้งกรณีลูกค้าเป็นเหยื่อและเป็นม้า

ป้องกันเหยื่อ

2 จัดการภัยทุจริตดิจิทัล

จัดการม้า

- **มาตรการ customer profiling** (กำหนดวงเงิน /แจ้งเตือนลูกค้า /อนุมัติวงเงินเพิ่มเติม)
- **ตรวจจับและรายงานบัญชีม้า** น้ำตาลเข้ม / น้ำตาลอ่อน
- **จัดการบัญชีม้า**ดำ เทาเข้ม เทาอ่อน น้ำตาลเข้ม น้ำตาลอ่อน ม้านิติที่มีผู้เกี่ยวข้องเป็นม้า ม้านิติบุคคลต้องสงสัยจากการตรวจ DBD และ ตำรวจ

3 ดูแลหลังเกิดภัยทุจริตดิจิทัล

การแก้ไขปัญหาและดูแลลูกค้า (Response)

- **ปลดระงับบัญชี/การให้บริการของผู้สุจริตโดยเร็ว**
- **มีกระบวนการตรวจสอบและเยียวยาความเสียหาย**

Enabler

กระบวนการแลกเปลี่ยนข้อมูล “ต้องแลกเปลี่ยนข้อมูลกับระบบ CFR ได้”

ส่งเสริมความรู้ทางการเงิน “ประชาชนไม่ตกเป็นเหยื่อมิจฉาชีพ”

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

4 Card Fraud Management : CFM

หลักการ ยกระดับความปลอดภัยในการใช้งานบัตร การบริหารจัดการภัยทุจริต และการดูแลประชาชนที่ได้รับความเสียหายจากภัยทุจริต

ขอบเขต ผู้ให้บริการออกบัตร (บัตรเครดิต บัตรเดบิต บัตร ATM และบัตร e-Money) | ผู้ให้บริการรับบัตร | ผู้ให้บริการเครือข่ายบัตร

ประเด็นสำคัญที่ยกระดับ

- การป้องกันความเสี่ยงจากการใช้บัตร และการดูแลช่วยเหลือลูกค้าเมื่อเกิดเหตุ
- ป้องกันภัยทุจริต และจัดการบัญชีม้า

I. ด้านธรรมาภิบาล

- **มีคณะทำงานหรือผู้บริหารระดับสูง** รับผิดชอบโดยตรง
- **กำหนดนโยบาย**การบริหารจัดการภัยทุจริตที่ชัดเจน
- **มีบุคลากร กระบวนการ เครื่องมือ** ที่เพียงพอและเหมาะสม
- **กำหนดเป้าหมาย ตัวชี้วัด ติดตามและประเมินผล** เช่น % ธุรกรรมที่ทุจริต จำนวนร้องเรียน

III. ด้านการรายงานข้อมูล

- รายงานข้อมูลต่อ ธปท.
- เปิดเผยข้อมูลการถูกเปรียบเทียบปรับหรือถูกกล่าวโทษ

* เรื่องสำคัญที่ปรับปรุงในครั้งนี้

II. ด้านการบริหารจัดการภัยทุจริต

1 การรู้จักและตรวจสอบข้อเท็จจริงลูกค้า

- **KYC** การเปิดใช้บริการ / **CDD** เมื่อทำธุรกรรมครั้งแรก

2 การติดตามและตรวจจับธุรกรรม

- **มีระบบติดตามตรวจจับ**ธุรกรรม 24x7
- **จัดระดับความเสี่ยงธุรกรรม และกำหนดเงื่อนไข**

3 การจัดการภัยทุจริต

- **มีการยืนยันตัวตน** ที่ปลอดภัย
  - ใช้ multi-factor authen. ยกเว้นธุรกรรมความเสี่ยงต่ำ
  - OTP format ให้สังเกตง่าย โดยแสดงจำนวนเงินก่อน
- **มีช่องทางให้ผู้ใช้บัตรบริหารความเสี่ยงได้เอง**: ปรับวงเงินธุรกรรม ระงับบัตรชั่วคราว อายัดบัตร ขอลดวงเงินสินเชื่อ
- **แจ้งเตือนการทำธุรกรรมทันที** โดยไม่มีค่าใช้จ่าย
- **ชะลอ และตรวจสอบกับผู้ใช้บัตรโดยเร็ว** เมื่อพบความผิดปกติ
- **ระงับการให้บริการบัตรที่เกี่ยวข้องกับบัญชีม้า**

4 การแก้ไขสถานการณ์และดูแลผู้ใช้บัตร

- **มีช่องทางติดต่อผู้ให้บริการ**เร่งด่วน 24x7
- **กำหนดกระบวนการช่วยเหลือดูแล และ SLA**
  - มีทีมงานที่เชี่ยวชาญ ขั้นตอนที่เป็นมาตรฐาน
  - ประสานงานผู้เกี่ยวข้องทันที เพื่อจำกัดความเสียหาย (ตั้งพักยอด กรณีบัตรเครดิต)
  - สื่อสารกับผู้ใช้บัตรอย่างต่อเนื่อง
  - แจ้งผลตรวจสอบ และเยียวยาความเสียหาย
    1) ผู้ใช้บัตรไม่ต้องรับผิดชอบและได้รับเยียวยา
       หากผู้ใช้บัตรไม่มีส่วนเกี่ยวข้อง
    2) ผู้ใช้บัตรอาจมีส่วนรับผิดชอบ หากผู้ใช้บัตรมีส่วนเกี่ยวข้อง โดยต้องชี้แจงเหตุให้ชัดเจน
       และมีกลไกอุทธรณ์
- **สื่อสารต่อสาธารณชน** ชี้แจงทำความเข้าใจและกำหนดแนวทางช่วยเหลือ กรณีเกิดภัยกับผู้ให้บริการหลายราย ที่กระทบความเชื่อมั่น

5 การสร้างความตระหนักรู้

เกี่ยวกับการใช้บริการบัตรที่สำคัญและภัยทุจริตในเชิงรุกผ่านช่องทางที่เข้าถึงได้ง่าย

6 ความร่วมมือระหว่างกัน

ผู้ให้บริการออกบัตร / ผู้ให้บริการรับบัตร:

- **แลกเปลี่ยนข้อมูลผ่านระบบ CFR** และสนับสนุนข้อมูลแก่พนักงานสอบสวน

ผู้ให้บริการเครือข่ายบัตร:

- **มีมาตรการสนับสนุนความปลอดภัย** ผ่าน scheme rule
- **ช่วยเหลือและสนับสนุนข้อมูลแก่สมาชิก** เพื่อป้องกันตรวจจับภัยทุจริต
- **มีช่องทางติดตามธุรกรรม**เพื่อช่วยเหลือผู้ถือบัตร
- **ไม่จำกัดหรือไม่บังคับใช้วิธีการยืนยันตัวตน** ที่อาจทำให้ผู้ใช้บริการมีความเสี่ยงเพิ่มขึ้น

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

5 Merchant Fraud Management : MFM

วัตถุประสงค์	**ยกระดับการจัดการความเสี่ยงร้านค้าในการรับชำระเงินผ่านช่องทางดิจิทัล เพื่อให้ประชาชนใช้บริการชำระเงินได้อย่างปลอดภัย**
บังคับใช้กับ	ผู้ให้บริการรับชำระเงินแทน, Acquirer, Payment Facilitator (PF) และ e-Money (ครอบคลุมทั้งบัญชีเงินฝาก บัญชี e-Money บัตรเดบิต บัตรเครดิต)
ประเด็นสำคัญที่ยกระดับ	• กำหนดมาตรฐานขั้นต่ำสำหรับ onboarding และการจัดการความเสี่ยงแบบ ongoing • ป้องกันภัยทุจริต และจัดการบัญชีม้า • ดูแล master & sub-merchant ทุกทอด

1 การกำหนดนโยบาย

- **กำหนดบทบาทหน้าที่ของคณะกรรมการหรือผู้บริหารระดับสูง**ในการกำหนดนโยบายการรับร้านค้า และการบริหารความเสี่ยง
- **การประเมินและติดตามความเสี่ยงร้านค้าที่เป็น platform/master merchant**
- **มีบุคลากร กระบวนการ เครื่องมือ** ในการจัดการภัยทุจริตที่เพียงพอกับจำนวน ขนาดร้านค้า
- **กำหนดเป้าหมาย ตัวชี้วัด ติดตามและประเมินผล** เช่น merchant fraud rate

2 กรอบการประเมินและจัดระดับความเสี่ยงร้านค้า

- **กำหนดมาตรฐานขั้นต่ำการประเมินความเสี่ยงร้านค้า** จากปัจจัยประเภทสินค้า/บริการ การทุจริต AML/CFT และปัจจัยอื่น เช่น business model, ปริมาณธุรกรรม
- **จัดระดับความเสี่ยงอย่างน้อย 3 ระดับ** คือ ร้านค้าทั่วไป ร้านค้าที่มีความเสี่ยงสูง ร้านค้าต้องห้าม
  - **ร้านค้าทั่วไป:** จัดกลุ่มตามลักษณะ/ขนาดร้านค้า
  - **ร้านค้าเสี่ยงสูง**: มีปัจจัยที่จะถูกใช้เป็นช่องทางทุจริต
  - **ร้านค้าต้องห้าม:** ร้านค้าผิด กม. หรือร้านที่มีรายชื่อ หรือมีเจ้าของผู้มีอำนาจจัดการ ผู้รับผลประโยชน์ที่แท้จริง เป็นเจ้าของบัญชีม้า

3 กระบวนการรู้จักและบริหารจัดการความเสี่ยงร้านค้า

- **Onboarding** สอดคล้องกับระดับความเสี่ยงร้านค้า และระบุ Merchant Category Code (MCC) ของร้านค้า
- **Merchant risk management**
  - มีกระบวนการและกลไก บริหารความเสี่ยงอย่างสม่ำเสมอ
  - มีแนวทางและกรอบเวลาดำเนินการ หากพบความผิดปกติ
  - ระงับการให้บริการ ระงับการ settle เงินเข้าบัญชีร้านค้าที่มีรายชื่อ หรือมีเจ้าของร้าน ผู้มีอำนาจจัดการร้านค้า หรือผู้รับผลประโยชน์ที่แท้จริง เป็นเจ้าของบัญชีม้า

ปฏิบัติตามมาตรฐานขั้นต่ำ สำหรับการ onboarding, merchant risk management, และการดูแล master merchant

4 การดำเนินการเมื่อเกิดเหตุภัยทุจริตฯ

- **มีกระบวนการแก้ไขสถานการณ์และดูแลร้านค้า** ที่ชัดเจน รวดเร็ว และเป็นธรรม

5 ความร่วมมือ

- **มีกลไกการแลกเปลี่ยนข้อมูลที่ถูกต้อง รวดเร็ว** และสนับสนุนข้อมูลให้กับหน่วยงานที่เกี่ยวข้อง

6 การสร้างความตระหนักรู้

- **สร้างความตระหนักรู้เกี่ยวกับภัยทุจริตดิจิทัล** ให้แก่ร้านค้าในเชิงรุก

* เรื่องสำคัญที่ปรับปรุงในครั้งนี้

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

มาตรฐานขั้นต่ำสำหรับ Merchant Fraud Management

เพื่อให้ผู้ประกอบธุรกิจใช้เป็นแนวทางกำหนดวิธีปฏิบัติในการบริหารจัดการความเสี่ยงร้านค้า ที่เหมาะสมกับระดับความเสี่ยงของร้านค้า แต่ไม่น้อยกว่ามาตรฐานขั้นต่ำ

	ร้านค้าทั่วไป		ร้านค้าเสี่ยงสูง
	ร้านค้าขนาดเล็ก (ยอดขาย ไม่เกิน 100,000 บาท*/เดือน)	**ร้านค้าทั่วไปอื่น ๆ** (ยอดขาย เกิน 100,000 บาท*/เดือน)	

1 Onboarding : การรู้จักร้านค้า

	ร้านค้าทั่วไป		ร้านค้าเสี่ยงสูง
Identification	รวบรวมข้อมูลและเอกสารหลักฐานแสดงตนของร้านค้า อย่างน้อยดังนี้ • ข้อมูลและเอกสารหลักฐานตามเกณฑ์ ปปง. + ข้อมูลร้านค้า/การประกอบธุรกิจ/ระยะเวลา เช่น ประเภทสินค้า/บริการ ภาพสินค้า • ชื่อผู้รับผลประโยชน์ที่แท้จริง (กรณีนิติบุคคล) • การคาดการณ์ยอดขายต่อเดือน/ปี • การรับรองตนเองโดยร้านค้าว่าขายสินค้าจริงตามที่ได้ให้ข้อมูลไว้	+ เอกสารเกี่ยวกับการประกอบธุรกิจเพิ่มเติม **เช่น** • นิติบุคคล : เอกสารจดทะเบียน DBD งบการเงิน • บุคคลธรรมดา : เอกสารการเสียภาษี ทะเบียนการค้า	
Verification	• ตรวจสอบความถูกต้อง ความแท้จริง ความเป็นปัจจุบันของข้อมูล ได้แก่ ข้อมูลตาม ปปง. ข้อมูลร้านค้า ชื่อบัญชีธนาคาร รายชื่อบัญชีม้า ผู้รับผลประโยชน์ที่แท้จริง (กรณีนิติบุคคล)	+ ตรวจสอบ blacklist ของเครือข่ายบัตร หรือแหล่งอื่น และ ตรวจสอบ location หน้าร้าน เช่น ผ่าน google map	
		+ **สุ่มตรวจสอบ** site visit หรือวิธีการเทียบเท่า site visit	+ site visit หรือ วิธีเทียบเท่า **ทุกราย** & ตรวจเพิ่มจากแหล่งข้อมูลที่น่าเชื่อถือ
ร้าน Online	• ตรวจสอบ URLs ว่าขายของจริง / IP address tracking (หากสงสัย อาจตรวจสอบเพิ่ม เช่น ขอหลักฐานการส่งของ, ตรวจชื่อ Domain owner		

2 Merchant Risk Management : การบริหารจัดการความเสี่ยงร้านค้าอย่างต่อเนื่อง

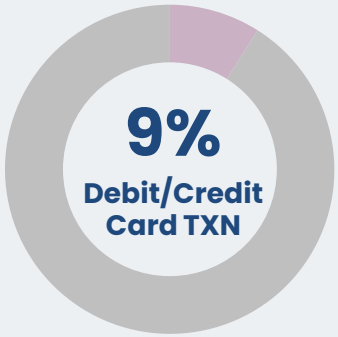
[1] ติดตาม ตรวจสอบ สถานะการดำเนินธุรกิจ • ด้านธุรกิจ เช่น ประเภทสินค้า ยอดขาย สถานที่ขาย ข้อมูลเจ้าของ ผู้มีอำนาจจัดการ หรือ ผู้รับผลประโยชน์ที่แท้จริง (กรณีนิติบุคคล) • ด้านความเสี่ยง เช่น การเปลี่ยนแปลงหรือความผิดปกติของธุรกรรมที่เพิ่มฉับพลัน สแกนข่าวเชิงลบ ตรวจรายชื่อ watch list **[2] ดำเนินการบริหารจัดการความเสี่ยง** : กำหนดวงเงินในการรับชำระเงิน / แนวทางและกรอบเวลาการดำเนินการในกรณีที่พบความผิดปกติ	**+ มีกระบวนการ ระบบงานที่มีเทคโนโลยีใช้ติดตามที่เข้มข้นขึ้น** เช่น การสุ่มตรวจแบบ mystery shopping, web crawler

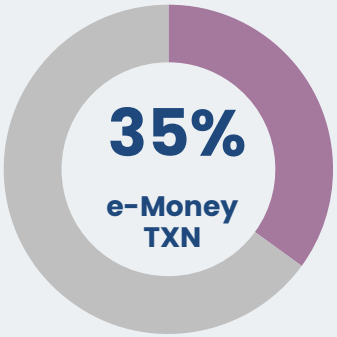
3 การดำเนินการสำหรับร้านค้าที่เป็น Master Merchant : e-Commerce platform, ผู้ประกอบธุรกิจรับชำระเงินทอดถัดไป

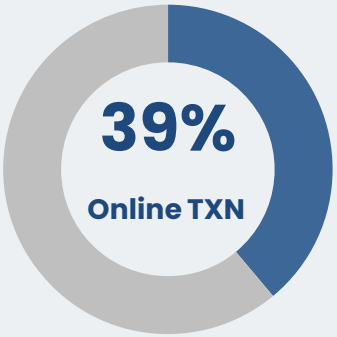
1. กำหนดหน้าที่และความรับผิดชอบระหว่างผู้ประกอบธุรกิจและ master merchant ให้ชัดเจนเป็นลายลักษณ์อักษร	2. กำหนดวิธีการในการดูแล master merchant ให้ชัดเจน เช่น นำส่งข้อมูลและตรวจสอบเพิ่มเติมเกี่ยวกับนโยบายการรับสมัคร sub-merchant และวิธีการตรวจสอบความน่าเชื่อถือของ sub-merchant	3. ผู้ประกอบธุรกิจอาจมีแนวทางบริหารความเสี่ยงอื่นทดแทน เช่น ให้ master merchant รับผิดชอบหากเกิดทุจริตจาก sub-merchant

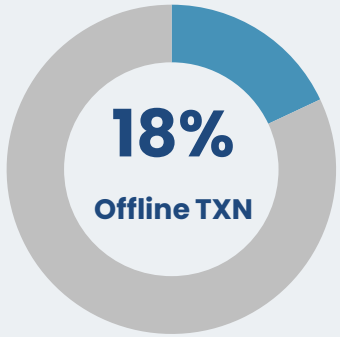
ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Payment Market Overview (2)









Bank's TXN Volume Growth*

22%	e-Money
8%	Acquirer & Payment Gateway
7%	Domestic Fund Transfer
22%	Cross-border Fund Transfer

Non-Bank's TXN Volume Growth*

15%	e-Money
20%	Acquirer & Payment Gateway
17%	Domestic Fund Transfer
232%	Cross-border Fund Transfer

As of September 2025
* Compare between 9M 2024 & 9M 2025