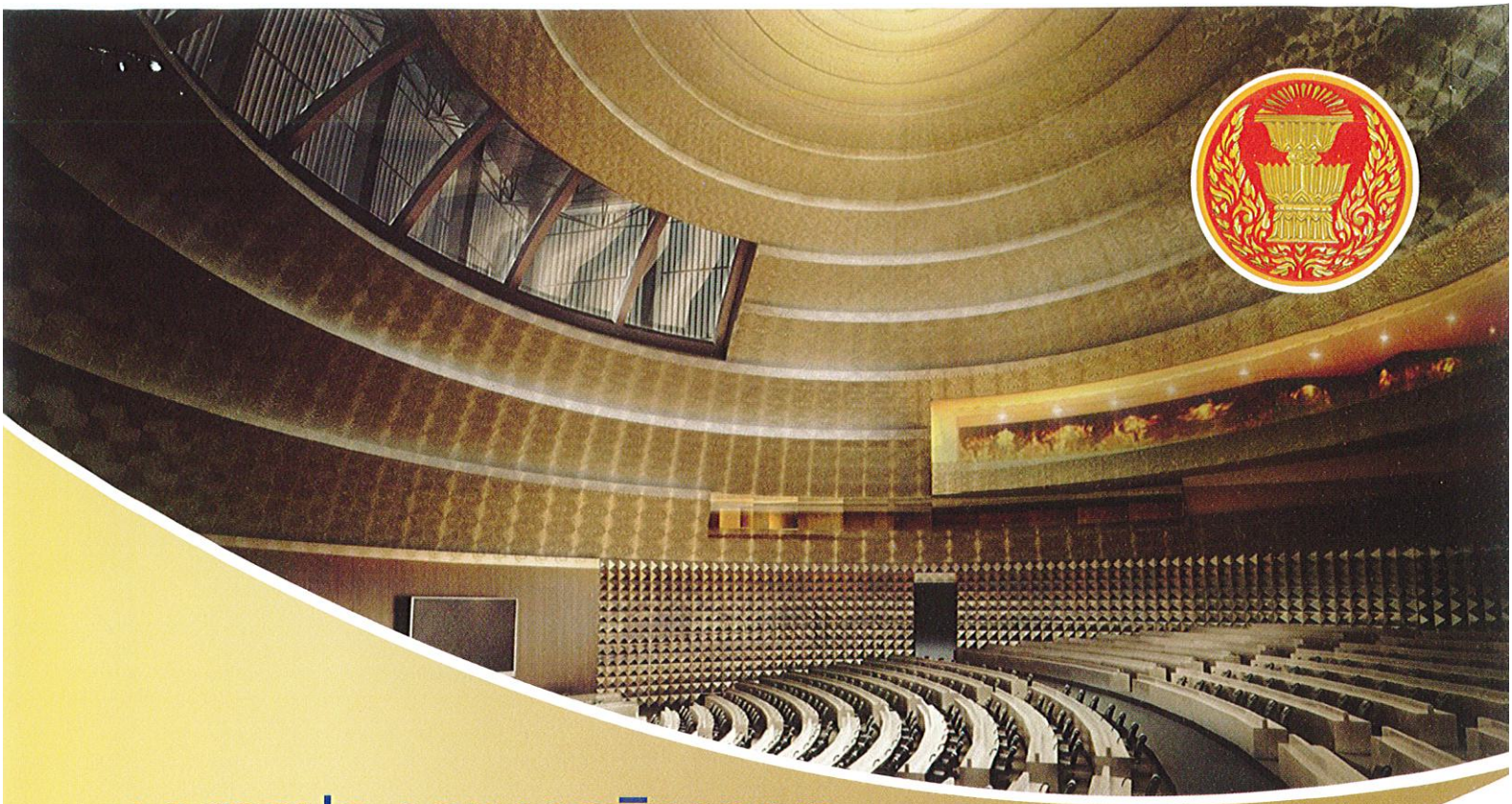

เอกสารประกอบการพิจารณา

พระราชกำหนดมาตรการป้องกันและปราบปราม อาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

อ.พ. 1/2568 สมัยวิสามัญ

อ.พ. 1/2568
สมัยวิสามัญ

สำนักวิชาการ
สำนักงานเลขาธิการสภาผู้แทนราษฎร
โทร 0 2242 5900 ต่อ 5730, 5740, 5750

พระราชกำหนดมาตรการป้องกันและปราบปราม
อาชญากรรมทางเทคโนโลยี (ฉบับที่ 2)
พ.ศ. 2568
(คณะรัฐมนตรี เป็นผู้เสนอ)

คำนำ

เอกสารประกอบการพิจารณา (อ.พ.) นี้ จัดทำขึ้นเพื่อประโยชน์ในการพิจารณาร่างพระราชบัญญัติประกอบรัฐธรรมนูญ ร่างพระราชบัญญัติ ญัตติขอแก้ไขเพิ่มเติมรัฐธรรมนูญ **พระราชกำหนด** ญัตติ หรือหนังสือสัญญาระหว่างประเทศ ที่เข้าสู่การประชุมของสภาผู้แทนราษฎร และที่ประชุมร่วมกันของรัฐสภา โดยศึกษา รวบรวมและวิเคราะห์ข้อมูล สถิติ ข้อเท็จจริง บทความทางวิชาการ และ/หรืองานวิจัยที่เกี่ยวข้อง เพื่อเป็นข้อมูลเบื้องต้นให้กับสมาชิกสภาผู้แทนราษฎร สมาชิกรัฐสภา กรรมาธิการ และบุคคลในวงงานรัฐสภา ใช้ในการประกอบการพิจารณาตลอดจนเป็นข้อมูลอ้างอิงสำหรับผู้ที่สนใจทั่วไป

สำนักวิชาการ
สำนักงานเลขาธิการสภาผู้แทนราษฎร

ผู้รับผิดชอบ

นายเชษฐา ทองยิ่ง	ผู้อำนวยการสำนักวิชาการ
นางสุภาวดี ตันตระกูล	ผู้บังคับบัญชากลุ่มงานบริการวิชาการ 2

ผู้จัดทำและรับผิดชอบ

นายณัฐพงศ์ พิมเสน	นิติกรชำนาญการ
นางสาวสุนันท์ เจสละ	เจ้าพนักงานธุรการอาวุโส
นางสาวสุพรรณิศา พรหมบุตร	เจ้าพนักงานธุรการชำนาญงาน

พฤษภาคม 2568

บทสรุปสำหรับสมาชิกสภาผู้แทนราษฎร

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 ตราขึ้นเพื่อรองรับภัยคุกคามทางเทคโนโลยีที่ซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว โดยมีเป้าหมายหลักในการปิดช่องทางการเงินที่ผิดกฎหมาย ป้องกันการฉ้อโกงออนไลน์ และเร่งรัดกระบวนการคืนเงินแก่ผู้เสียหาย โดยครอบคลุมสาระสำคัญใน 6 ด้าน ดังนี้

1. ควบคุมธุรกรรมการเงินและสินทรัพย์ดิจิทัล

ขยายความหมาย “ผู้ประกอบธุรกิจ” ให้ครอบคลุมถึงผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล พร้อมทั้งกำหนดนิยาม “กระเป๋าสินทรัพย์ดิจิทัล” และ “บัญชีเงินอิเล็กทรอนิกส์” เพื่อใช้ในการตรวจสอบและสกัดเส้นทางการเงินที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี นอกจากนี้ หน่วยงานรัฐสามารถเข้าถึงข้อมูลบัญชีและธุรกรรมของลูกค้าเมื่อมีเหตุสงสัย และสถาบันการเงินหรือผู้ประกอบธุรกิจต้องปฏิเสธการเปิดบัญชี ระงับการให้บริการหรือการทำธุรกรรมหรือปิดบัญชีกับบุคคลที่มีรายชื่อหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยีที่ ศปอท. ประกาศได้ทันที

2. ควบคุมการใช้บริการโทรคมนาคม

กำหนดให้ผู้ให้บริการโทรศัพท์ต้องคัดกรองข้อความการบริการสารสั้น (SMS) ที่อาจเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี และเปิดทางให้หน่วยงานรัฐสามารถสั่งระงับการให้บริการโทรคมนาคมได้ทันทีเมื่อพบหลักฐานว่ามีการใช้โทรคมนาคมในการกระทำความผิด

3. คืนเงินแก่ผู้เสียหายอย่างเป็นระบบ

กำหนดขั้นตอนการคืนเงินอย่างเป็นระบบ ตั้งแต่การรายงาน ตรวจสอบ ประกาศบัญชีของบุคคลซึ่งเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีและการแจ้งให้ผู้เสียหายและผู้เกี่ยวข้องกับบัญชียื่นคำร้องและหลักฐานที่เกี่ยวข้อง รวมถึงการพิจารณาคืนเงินให้ผู้เสียหายโดยคณะกรรมการธุรกรรม พร้อมเปิดโอกาสให้ผู้เสียหายอุทธรณ์ได้ตามสิทธิและในกรณีไม่มีผู้เสียหายหรือผู้ที่เกี่ยวข้องมายื่นคำร้องภายใน 10 ปี เงินในบัญชีจะตกเป็นของกองทุนป้องกันและปราบปรามการฟอกเงิน แต่สามารถขอคืนได้หากมีเหตุอันควร

4. จัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.)

จัดตั้งศูนย์เฉพาะกิจภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่รับแจ้งเหตุ ตรวจสอบธุรกรรมต้องสงสัย บูรณาการข้อมูลกับหน่วยงานที่เกี่ยวข้อง และรายงานผลการดำเนินงานเป็นประจำ

5. เพิ่มความรับผิดของผู้ให้บริการ

กำหนดให้สถาบันการเงิน ผู้ให้บริการโทรคมนาคม และผู้ให้บริการสื่อสังคมออนไลน์ต้องร่วมรับผิดชอบต่อความเสียหายที่เกิดจากอาชญากรรมทางเทคโนโลยีหากไม่ปฏิบัติตามมาตรฐานป้องกันที่กำหนด เว้นแต่สามารถพิสูจน์ได้ว่าปฏิบัติตามมาตรฐานที่กำหนดแล้ว

6. คุ้มครองข้อมูลส่วนบุคคลและผู้ถึงแก่กรรม

ห้ามมิให้มีการใช้ จัดเก็บ หรือเผยแพร่ข้อมูลส่วนบุคคลและผู้ถึงแก่กรรมเพื่อนำไปใช้ในการกระทำความผิดโดยมีบทลงโทษทั้งจำคุกและปรับ มาตรการนี้มีขึ้นเพื่อป้องกันการแอบอ้างและการเปิดบัญชีโดยไม่ชอบ

ดังนั้น พระราชกำหนดฉบับนี้ได้วางกรอบการจัดการอาชญากรรมทางเทคโนโลยีทั้งในเชิงป้องกัน ระงับเหตุ และเยียวยาผู้เสียหาย โดยเน้นการทำงานเชิงรุก การบูรณาการข้อมูล และการมีส่วนร่วมของทุกภาคส่วน เพื่อเพิ่มประสิทธิภาพในการคุ้มครองประชาชนจากอาชญากรรมทางเทคโนโลยีอย่างยั่งยืน

เอกสารประกอบการพิจารณา

สารบัญ

	หน้า
บทสรุปสำหรับสมาชิกสภาผู้แทนราษฎร	**ก**
ส่วนที่ 1	
- หลักการและเหตุผลพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)	1-1
- สรุปสาระสำคัญพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)	1-3
- ตารางเปรียบเทียบพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 กับพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)	1-10
ส่วนที่ 2 บทวิเคราะห์	2-1
ส่วนที่ 3 ข้อมูลประกอบการพิจารณา	3-1
1. เทคโนโลยีการยืนยันตัวตน	3-1
2. การปราบปรามอาชญากรรมทางเทคโนโลยีของภาครัฐ	3-4
3. มาตรการทางกฎหมายแก้ไขปัญหามิจฉาชีพออนไลน์ของประเทศต่าง ๆ	3-7

ส่วนที่ 1

หลักการและเหตุผล

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2)

พ.ศ. 2568

(คณะรัฐมนตรี เป็นผู้เสนอ)

<u>หลักการ</u>

แก้ไขเพิ่มเติมพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ดังนี้

(1) แก้ไขเพิ่มเติมบทนิยามคำว่า “ผู้ประกอบธุรกิจ” และเพิ่มบทนิยามคำว่า “กระเป๋าสินทรัพย์ดิจิทัล” และ “บัญชีเงินอิเล็กทรอนิกส์” (แก้ไขเพิ่มเติมมาตรา 3)

(2) แก้ไขเพิ่มเติมให้สถาบันการเงินและผู้ประกอบธุรกิจมีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับเลขที่กระเป๋าสินทรัพย์ดิจิทัล (แก้ไขเพิ่มเติมมาตรา 4 วรรคหนึ่ง)

(3) เพิ่มบทบัญญัติให้หน่วยงานที่มีหน้าที่กำกับดูแลสถาบันการเงิน ผู้ประกอบธุรกิจ ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น ผู้ให้บริการอื่นที่เกี่ยวข้อง และผู้ให้บริการสื่อสังคมออนไลน์กำหนดมาตรฐานหรือมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยี (เพิ่มมาตรา 4/1)

(4) เพิ่มบทบัญญัติเพื่อการควบคุมการเปิดบัญชี ระงับการให้บริการหรือการทำธุรกรรม หรือปิดบัญชีกับบุคคลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี (เพิ่มมาตรา 4/2)

(5) เพิ่มบทบัญญัติเกี่ยวกับการระงับการให้บริการโทรคมนาคมที่ใช้ในการกระทำความผิดอาชญากรรมทางเทคโนโลยี (เพิ่มมาตรา 5 วรรคสองและวรรคสาม)

(6) เพิ่มบทบัญญัติเกี่ยวกับการระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์หรือนำข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายออกจากระบบคอมพิวเตอร์ในกรณีที่มีการประกอบธุรกิจสินทรัพย์ดิจิทัลโดยไม่ได้รับอนุญาต (เพิ่มมาตรา 7/1)

(7) เพิ่มบทบัญญัติเกี่ยวกับการคืนเงินแก่ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี (เพิ่มมาตรา 8/1 มาตรา 8/2 มาตรา 8/3 และมาตรา 8/4)

(8) เพิ่มบทบัญญัติให้มีการจัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) (เพิ่มมาตรา 8/5 มาตรา 8/6 มาตรา 8/7 มาตรา 8/8 และมาตรา 8/9)

(9) เพิ่มบทบัญญัติเกี่ยวกับความรับผิดทางแพ่งของสถาบันการเงินหรือผู้ประกอบธุรกิจ ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น ผู้ให้บริการอื่นที่เกี่ยวข้อง หรือผู้ให้บริการสื่อสังคมออนไลน์ในความเสียหายที่เกิดจากอาชญากรรมทางเทคโนโลยี (เพิ่มมาตรา 8/10)

(10) เพิ่มบทกำหนดโทษอาญากรณีการไม่ปฏิบัติตามมาตรา 4/2 การไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ตามมาตรา 7/1 การลงทะเบียนเพื่อใช้บริการโทรศัพท์ไม่ถูกต้องครบถ้วน การกระทำความผิดต่อข้อมูลเกี่ยวกับบุคคลหรือผู้ถึงแก่กรรม (เพิ่มมาตรา 8/11 มาตรา 8/12 มาตรา 11/1 และมาตรา 11/2)

<u>เหตุผล</u>

โดยที่ปรากฏว่ามีการนำเงินที่ได้จากการกระทำความผิดอาชญากรรมทางเทคโนโลยีไปซื้อขายสินทรัพย์ดิจิทัลซึ่งทำให้ยากต่อการตรวจสอบการทำธุรกรรมและการระงับการทำธุรกรรม การใช้บริการโทรคมนาคมเพื่อกระทำความผิดอาชญากรรมทางเทคโนโลยี และการนำข้อมูลของบุคคลหรือผู้ถึงแก่กรรมมาใช้ในการกระทำความผิดดังกล่าว สมควรกำหนดมาตรการเพิ่มเติมในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีในกรณีดังกล่าว และจัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี รวมทั้งกำหนดกระบวนการการคืนเงินแก่ผู้เสียหายให้เป็นไปโดยเร็ว และการมีส่วนร่วมรับผิดชอบในความเสียหายที่เกิดจากการกระทำความผิดอาชญากรรมทางเทคโนโลยีเพื่อเยียวยาผู้เสียหายตลอดจนการกำหนดโทษในส่วนที่เกี่ยวข้อง จึงเป็นกรณีฉุกเฉินที่มีความจำเป็นรีบด่วนอันมิอาจจะหลีกเลี่ยงได้เพื่อประโยชน์ในอันที่จะต้องมีมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีดังกล่าวเพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในทางเศรษฐกิจของประเทศจึงจำเป็นต้องตราพระราชกำหนดนี้

สรุปสาระสำคัญ
พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2)
พ.ศ. 2568
(คณะรัฐมนตรี เป็นผู้เสนอ)

---

1. ชื่อพระราชกำหนด

พระราชกำหนดนี้เรียกว่า “พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 ” (มาตรา 1)

2. วันที่มีผลใช้บังคับ

พระราชกำหนดนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป (มาตรา 2)

3. ยกเลิกและบัญญัติบทนิยามคำว่า “ผู้ประกอบธุรกิจ”

ให้ยกเลิกความในบทนิยามคำว่า “ผู้ประกอบธุรกิจ” ในมาตรา 3 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และให้ใช้ความต่อไปนี้แทน

““ผู้ประกอบธุรกิจ” หมายความว่า ผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงินและผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลตามกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล” (มาตรา 3)

4. เพิ่มบทนิยามคำว่า “กระเป๋าสินทรัพย์ดิจิทัล” และ “บัญชีเงินอิเล็กทรอนิกส์”

ให้เพิ่มความต่อไปนี้เป็นบทนิยามต่อจากบทนิยามคำว่า “ผู้ประกอบธุรกิจ” ในมาตรา 3 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

““กระเป๋าสินทรัพย์ดิจิทัล” หมายความว่า ระบบที่ใช้ในการจัดเก็บสินทรัพย์ดิจิทัล (wallet)”

“บัญชีเงินอิเล็กทรอนิกส์” หมายความรวมถึงบัญชีสินทรัพย์ดิจิทัล” (มาตรา 4)

5. กำหนดให้กรณีที่มีเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงินและผู้ประกอบธุรกิจต้องเปิดเผยหรือแลกเปลี่ยนข้อมูลบัญชี ธุรกรรม และเลขที่กระเป๋าสินทรัพย์ดิจิทัลของลูกค้าผ่านระบบกลางที่หน่วยงานที่เกี่ยวข้องเห็นชอบร่วมกัน

ให้ยกเลิกความในวรรคหนึ่งของมาตรา 4 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และให้ใช้ความต่อไปนี้แทน

“มาตรา 4 เพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ในกรณีที่มีเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงินและผู้ประกอบธุรกิจมีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าที่เกี่ยวข้อง และเลขที่กระเป๋าสินทรัพย์ดิจิทัลในระหว่างสถาบันการเงินและผู้ประกอบธุรกิจนั้นผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน ธนาคารแห่งประเทศไทย และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ เห็นชอบร่วมกัน” (มาตรา 4)

6. กำหนดหน่วยงานที่ต้องจัดทำมาตรการป้องกันอาชญากรรมทางเทคโนโลยี การคัดกรอง SMS ที่อาจเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี และกำหนดมาตรการป้องกันการเปิดบัญชีและระงับการให้บริการหรือการทำธุรกรรมหรือปิดบัญชีกับบุคคลที่มีรายชื่อเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี

ให้เพิ่มความต่อไปนี้เป็นมาตรา 4/1 และมาตรา 4/2 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

“มาตรา 4/1 เพื่อประโยชน์แห่งมาตรา 8/10 ให้ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ และคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กำหนดมาตรฐานหรือมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยี

ให้ผู้ให้บริการเครือข่ายโทรศัพท์และผู้ให้บริการโทรคมนาคมอื่นมีหน้าที่ตรวจสอบเพื่อคัดกรองเนื้อหาการบริการสารสั้น (SMS) ที่อาจเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีตามมาตรฐานหรือมาตรการที่สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติกำหนดตามวรรคหนึ่ง

มาตรา 4/2 เมื่อ ศปอท. ได้แจ้งรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยีตามประกาศในมาตรา 8/5 (6) ให้สถาบันการเงินหรือผู้ประกอบธุรกิจปฏิเสธการเปิดบัญชี ระงับการให้บริการหรือการทำธุรกรรม หรือปิดบัญชี กับบุคคลที่มีรายชื่อหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลดังกล่าว จนกว่าจะมีการเพิกถอนรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลนั้น” (มาตรา 6)

7. กำหนดให้หน่วยงานที่บังคับใช้กฎหมายต้องแจ้งสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เพื่อสั่งระงับบริการโทรคมนาคมทันที หากมีหลักฐานอันควรเชื่อได้ว่ามีการใช้บริการโทรคมนาคมเพื่อกระทำความผิดอาชญากรรมทางเทคโนโลยี

ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา 5 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

“ในกรณีที่ปรากฏพยานหลักฐานอันควรเชื่อได้ว่ามีการใช้บริการโทรคมนาคมเพื่อกระทำความผิดอาชญากรรมทางเทคโนโลยีไม่ว่าจะปรากฏจากการตรวจสอบข้อมูลตามวรรคหนึ่ง หรือพยานหลักฐานอื่นใด ให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน หรือ ศปอท. แล้วแต่กรณี แจ้งให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติสั่งให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องกับการกระทำนั้นระงับการให้บริการโทรคมนาคมดังกล่าว

การยกเลิกการระงับการให้บริการตามวรรคสอง ให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ และ ศปอท. เห็นชอบร่วมกัน” (มาตรา 7)

8. กำหนดให้เจ้าหน้าที่ที่ได้รับแต่งตั้งตามกฎหมาย มีอำนาจสั่งระงับการเผยแพร่ข้อมูลหรือลบข้อมูลผิดกฎหมายออกจากระบบคอมพิวเตอร์ทันที หากพบผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลโดยไม่ได้รับอนุญาต โดยให้ดำเนินการตามขั้นตอนที่รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมประกาศกำหนด

ให้เพิ่มความต่อไปนี้เป็นมาตรา 7/1 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

“มาตรา 7/1 เมื่อความปรากฏต่อพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ว่ามีผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลโดยไม่ได้รับอนุญาตตามกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล ให้พนักงานเจ้าหน้าที่ดังกล่าวมีคำสั่งระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์หรือนำข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายออกจากระบบคอมพิวเตอร์โดยพลัน

การสั่งระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์หรือนำข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายออกจากระบบคอมพิวเตอร์ตามวรรคหนึ่ง ให้ดำเนินการตามขั้นตอนที่รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมประกาศกำหนด” (มาตรา 8)

9. เพิ่มบทบัญญัติเกี่ยวกับการคืนเงินแก่ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี

ให้เพิ่มความต่อไปนี้เป็นมาตรา 8/1 มาตรา 8/2 มาตรา 8/3 มาตรา 8/4 มาตรา 8/5 มาตรา 8/6 มาตรา 8/7 มาตรา 8/8 มาตรา 8/9 มาตรา 8/10 มาตรา 8/11 และมาตรา 8/12 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ดังนี้

9.1 กำหนดให้มีการบูรณาการข้อมูลและการปฏิบัติงานระหว่างหน่วยงานที่เกี่ยวข้อง เพื่อคืนเงินแก่ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี

“มาตรา 8/1 เพื่อประโยชน์ในการคืนเงินแก่ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี ให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ หรือสถาบันการเงินหรือผู้ประกอบธุรกิจรายงานข้อมูลเกี่ยวกับการทำธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ไปยังสำนักงานป้องกันและปราบปรามการฟอกเงิน

ในการตรวจสอบรายงานตามวรรคหนึ่ง ให้เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินมอบหมายพนักงานเจ้าหน้าที่ตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินเป็นพนักงานเจ้าหน้าที่ผู้รับผิดชอบ และอาจขอให้หน่วยงานของรัฐ สถาบันการเงินหรือผู้ประกอบธุรกิจที่เกี่ยวข้องให้ความช่วยเหลือ สนับสนุน หรือเข้าร่วมปฏิบัติหน้าที่ตามความเหมาะสมก็ได้

หน่วยงานของรัฐ สถาบันการเงินหรือผู้ประกอบธุรกิจตามวรรคสอง ต้องให้ความช่วยเหลือ สนับสนุน หรือมอบหมายบุคคลเข้าร่วมปฏิบัติหน้าที่ตามสมควรแก่กรณี และให้บุคคลที่ได้รับมอบหมายเข้าร่วมปฏิบัติหน้าที่ได้รับค่าตอบแทนตามระเบียบที่เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินกำหนดโดยได้รับความเห็นชอบของกระทรวงการคลัง

การรายงานและการตรวจสอบรายงานให้เป็นไปตามหลักเกณฑ์ วิธีการ เงื่อนไข และระยะเวลาที่กำหนดในกฎกระทรวง

9.2 กำหนดกระบวนการคืนเงินแก่ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี โดยกำหนดขั้นตอนหลัก 3 ประการ ได้แก่ 1. ขั้นตอนประกาศข้อมูลบัญชีและยื่นคำร้อง 2. ขั้นตอนตรวจสอบคำร้องและคืนเงิน 3. ขั้นตอนอุทธรณ์

มาตรา 8/2 เมื่อสำนักงานป้องกันและปราบปรามการฟอกเงินได้ตรวจสอบรายงานตามมาตรา 8/1 แล้ว ให้ประกาศข้อมูลบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลซึ่งเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีในราชกิจจานุเบกษา และในประกาศดังกล่าว ให้แจ้งผู้เสียหายให้ยื่นคำร้องพร้อมแสดงหลักฐานแห่งความเสียหาย และแจ้งผู้ที่เกี่ยวข้องกับบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ ให้ยื่นคำร้องคัดค้านพร้อมแสดงหลักฐานว่าเงินในบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวไม่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ภายในเก้าสิบวันนับแต่วันที่ประกาศในราชกิจจานุเบกษา ในกรณีการแจ้งผู้เสียหายนั้น หากทราบตัวผู้เสียหายที่ชัดเจนแน่นอน ให้แจ้งให้ผู้เสียหายนั้นทราบโดยตรงอีกทางหนึ่งด้วย

เมื่อพนักงานเจ้าหน้าที่ได้ตรวจสอบคำร้องตามวรรคหนึ่งแล้ว ให้พนักงานเจ้าหน้าที่เสนอเรื่องต่อคณะกรรมการธุรกรรมตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และให้คณะกรรมการธุรกรรมตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินมีอำนาจสั่งคืนเงินให้แก่ผู้เสียหาย

การแจ้ง การยื่นคำร้อง การตรวจสอบคำร้อง การเสนอเรื่อง และการพิจารณาคืนเงินให้แก่ผู้เสียหาย การแจ้งผลการพิจารณาต่อผู้เสียหายและผู้ที่เกี่ยวข้อง และวิธีการคืนเงินให้แก่ผู้เสียหาย ให้เป็นไปตามหลักเกณฑ์ วิธีการ เงื่อนไข และระยะเวลาที่กำหนดในกฎกระทรวง

ในกรณีที่ผู้เสียหายหรือผู้ที่เกี่ยวข้องไม่เห็นด้วยกับคำสั่งของคณะกรรมการธุรกรรมตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ให้ยื่นคำร้องต่อศาลแพ่งภายในสามสิบวันนับแต่วันที่ได้รับแจ้งผลการพิจารณา และให้นำหมวด 6 การดำเนินการเกี่ยวกับทรัพย์สิน แห่งพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาใช้บังคับโดยอนุโลม คำพิพากษาของศาลอุทธรณ์ให้เป็นที่สุด

9.3 กำหนดให้หากสำนักงานป้องกันและปราบปรามการฟอกเงิน พบเหตุอันควรสงสัยหรือได้รับข้อมูลจากระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลว่ามีเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีเพื่อให้ผู้เสียหายได้รับเงินคืนจากเหตุอาชญากรรมนั้น ให้มีการบูรณาการข้อมูล และการปฏิบัติงานระหว่างหน่วยงานที่เกี่ยวข้องและดำเนินการตามกระบวนการคืนเงินแก่ผู้เสียหาย

มาตรา 8/3 ให้นำมาตรา 8/1 และมาตรา 8/2 มาใช้บังคับแก่กรณีที่สำนักงานป้องกันและปราบปรามการฟอกเงินพบเหตุอันควรสงสัยเองหรือได้รับข้อมูลจากระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา 4 ด้วยโดยอนุโลม

9.4 กำหนดเงื่อนไขการให้เงินในบัญชีตกเป็นของกองทุนป้องกันและปราบปรามการฟอกเงินและสิทธิขอคืนเงิน

มาตรา 8/4 ในกรณีปรากฏข้อเท็จจริงว่าบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ใด ไม่มีผู้เสียหายหรือผู้ที่เกี่ยวข้องมายื่นคำร้องภายในสิบปีนับแต่วันที่ครบกำหนดตามมาตรา 8/2 หรือปรากฏข้อเท็จจริงว่าได้คืนเงินให้แก่ผู้เสียหายแล้วแต่ยังมีเงินเหลืออยู่ในบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ ให้เงินในบัญชีเงินฝาก

หรือบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวตกเป็นของกองทุนป้องกันและปราบปรามการฟอกเงิน แต่ไม่ตัดสิทธิเจ้าของเงินหรือเจ้าของบัญชีที่จะขอรับเงินคืนจากกองทุนป้องกันและปราบปรามการฟอกเงินภายหลังจากนั้น ถ้าพิสูจน์ได้ว่าตนมีเหตุอันสมควรที่ไม่อาจมารับคืนได้ภายในกำหนดเวลาดังกล่าว ในกรณีเช่นนั้น ให้คืนเงินให้แก่ผู้นั้น

10. เพิ่มบทบัญญัติให้มีการจัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.)

10.1 กำหนดให้มีศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

มาตรา 8/5 ให้จัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เรียกโดยย่อว่า “ศปอท.” ในสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีหน้าที่และอำนาจดังต่อไปนี้

(1) รับแจ้งเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยีจากผู้เสียหาย และให้ถือว่าการแจ้งเหตุดังกล่าวเป็นการร้องทุกข์โดยวิธีการทางอิเล็กทรอนิกส์ตามมาตรา 8 วรรคสอง

(2) ระงับการทำธุรกรรมที่เป็นบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ที่ปรากฏพยานหลักฐานอันควรเชื่อได้ว่าเกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยีโดยทันที หรือเพิกถอนการระงับการทำธุรกรรมดังกล่าวในกรณีที่พิสูจน์ได้ว่ามิได้เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี

(3) สั่งให้สถาบันการเงินหรือผู้ประกอบธุรกิจนำส่งข้อมูลเกี่ยวกับบัญชีและธุรกรรมที่ต้องสงสัย

(4) รวบรวมจำนวนบัญชีเงินฝากที่บุคคลใดถือไว้ เพื่อประโยชน์ในการตรวจสอบว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยี แต่ทั้งนี้ ไม่รวมถึงจำนวนเงินฝากทั้งหมดหรือของแต่ละบัญชี

(5) เปิดเผยหรือแลกเปลี่ยนข้อมูลที่เกี่ยวข้องเพื่อประโยชน์ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีกับหน่วยงานของรัฐและหน่วยงานเอกชนที่เกี่ยวข้อง

(6) ประกาศรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี และเพิกถอนรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลดังกล่าว ทั้งนี้ตามหลักเกณฑ์ที่ ศปอท. ประกาศกำหนด

(7) แจ้งข้อมูลหมายเลขโทรศัพท์ บริการสารสั้น (SMS) หรือชื่อผู้ส่งสารสั้น หรือข้อมูลการใช้บริการโทรคมนาคมอื่น ให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติทราบ เพื่อดำเนินการตามมาตรา 5 วรรคสอง

(8) รวบรวมข้อมูลเกี่ยวกับอาชญากรรมทางเทคโนโลยีเพื่อปฏิบัติการตามพระราชกำหนดนี้

(9) จัดทำรายงานผลการดำเนินการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเสนอคณะกรรมการตามมาตรา 13 เดือนละหนึ่งครั้ง

10.2 กำหนดให้หน่วยงานรัฐที่ระบุไว้หรือหน่วยงานอื่นของรัฐหรือหน่วยงานเอกชนที่รัฐมนตรีกำหนดต้องแต่งตั้งผู้แทนเข้าร่วมปฏิบัติงานในศูนย์ ศปอท. เพื่อสนับสนุนการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

มาตรา 8/6 ให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือหน่วยงานอื่นของรัฐหรือหน่วยงานของเอกชนที่รัฐมนตรีประกาศกำหนด แต่งตั้งผู้แทนเข้าร่วมปฏิบัติงานใน ศปอท.

10.3 กำหนดให้คณะกรรมการตามมาตรา 13 แต่งตั้งหัวหน้า ศปอท. รับผิดชอบบริหารงาน เป็นผู้แทนติดต่อกับบุคคลภายนอก และปฏิบัติหน้าที่ตามที่พระราชกำหนดนี้กำหนดหรือคณะกรรมการตามมาตรา 13 มอบหมาย โดยรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อาจวางระเบียบการปฏิบัติงานของ ศปอท. เพิ่มเติมได้

มาตรา 8/7 ให้คณะกรรมการตามมาตรา 13 แต่งตั้งหัวหน้า ศปอท. โดยมีหน้าที่และอำนาจดังต่อไปนี้

(1) รับผิดชอบในการบริหารงานของ ศปอท.

(2) เป็นผู้แทนของ ศปอท. ในการติดต่อกับบุคคลภายนอก

(3) ปฏิบัติหน้าที่อื่นตามที่กำหนดไว้ในพระราชกำหนดนี้

(4) ปฏิบัติการอื่นตามที่คณะกรรมการตามมาตรา 13 มอบหมาย

มาตรา 8/8 รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอาจวางระเบียบการปฏิบัติงานของ ศปอท. ก็ได้

10.4 กำหนดให้เจ้าหน้าที่ ศปอท. ได้รับค่าตอบแทนตามระเบียบที่รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมประกาศกำหนด โดยความเห็นชอบของกระทรวงการคลัง

มาตรา 8/9 ให้เจ้าหน้าที่ซึ่งได้รับการแต่งตั้งให้ปฏิบัติงานใน ศปอท. ได้รับค่าตอบแทนตามระเบียบที่รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมประกาศกำหนด โดยความเห็นชอบของกระทรวงการคลัง

11. กำหนดให้สถาบันการเงินหรือผู้ประกอบธุรกิจ ผู้ให้บริการโทรคมนาคมและสื่อสังคมออนไลน์ต้องร่วมรับผิดชอบความเสียหายจากอาชญากรรมทางเทคโนโลยี เว้นแต่พิสูจน์ได้ว่าได้ปฏิบัติตามมาตรฐานหรือมาตรการป้องกันตามที่หน่วยงานที่เกี่ยวข้องกำหนดแล้ว

มาตรา 8/10 ให้สถาบันการเงินหรือผู้ประกอบธุรกิจ ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น ผู้ให้บริการอื่นที่เกี่ยวข้อง หรือผู้ให้บริการสื่อสังคมออนไลน์ มีส่วนร่วมรับผิดชอบในความเสียหายที่เกิดจากอาชญากรรมทางเทคโนโลยี เว้นแต่จะพิสูจน์ได้ว่าสถาบันการเงินหรือผู้ประกอบธุรกิจ ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น ผู้ให้บริการอื่นที่เกี่ยวข้อง หรือผู้ให้บริการสื่อสังคมออนไลน์ได้ปฏิบัติตามมาตรฐานหรือมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีที่กำหนดโดยธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ แล้วแต่กรณี

12. เพิ่มบทกำหนดโทษอาญากรณีการไม่ปฏิบัติตามมาตรา 4/2 การไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ตามมาตรา 7/1 การลงทะเบียนเพื่อใช้บริการโทรศัพท์ไม่ถูกต้องครบถ้วน การกระทำความผิดต่อข้อมูลเกี่ยวกับบุคคลหรือผู้ถึงแก่กรรม

12.1 กำหนดบทลงโทษสำหรับสถาบันการเงินหรือผู้ประกอบธุรกิจที่ไม่ปฏิบัติตาม มาตรา 4/2 และกำหนดบทลงโทษสำหรับผู้ที่ไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ ตามมาตรา 7/1

มาตรา 8/11 สถาบันการเงินหรือผู้ประกอบธุรกิจใดไม่ปฏิบัติตามมาตรา 4/2 ต้องระวางโทษปรับไม่เกินห้าแสนบาท

ในกรณีที่การกระทำความผิดตามวรรคหนึ่งเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 8/12 ผู้ใดไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ตามมาตรา 7/1 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ” (มาตรา 9)

12.2 กำหนดโทษกรณีลงทะเบียนหมายเลขโทรศัพท์ไม่ถูกต้อง โดยรู้หรือควรรู้ว่าเลขหมายจะถูกใช้เพื่ออาชญากรรมทางเทคโนโลยี รวมไปถึงการใช้ เก็บรวบรวม เปิดเผยข้อมูลที่ระบุตัวบุคคล หรือผู้เสียชีวิตเพื่อก่ออาชญากรรมทางเทคโนโลยีหรือความผิดอื่น

ให้เพิ่มความต่อไปนี้เป็นมาตรา 11/1 และมาตรา 11/2 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

มาตรา 11/1 ในกรณีที่ผู้ซื้อเลขหมายโทรศัพท์ลงทะเบียนเพื่อใช้บริการ หรือผู้ขายเลขหมายโทรศัพท์ที่มีหน้าที่เกี่ยวกับการลงทะเบียนให้แก่ผู้ใช้บริการ ลงทะเบียนไม่ถูกต้องครบถ้วนตามที่คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติกำหนด โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 11/2 ผู้ใดใช้ข้อมูลเกี่ยวกับบุคคลหรือผู้ถึงแก่กรรมซึ่งทำให้สามารถระบุตัวบุคคลหรือผู้ถึงแก่กรรมนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เพื่อกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ผู้ใดเก็บรวบรวม ครอบครอง หรือเปิดเผยข้อมูลเกี่ยวกับบุคคลหรือผู้ถึงแก่กรรมซึ่งทำให้สามารถระบุตัวบุคคลหรือผู้ถึงแก่กรรมนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เพื่อนำไปใช้หรือให้บุคคลอื่นใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษตามที่บัญญัติในวรรคหนึ่ง

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสองได้กระทำโดยซื้อ เสนอซื้อ ขาย เสนอขาย แลกเปลี่ยน เสนอแลกเปลี่ยน หรือแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ” (มาตรา 10)

ตารางเปรียบเทียบ

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 กับพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
พระราชกำหนด **มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี** **พ.ศ. 2566** ————————	**พระราชกำหนด** **มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2)** **พ.ศ. 2568** ———————— พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พระราชกำหนดนี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา 26 ประกอบกับมาตรา 32 มาตรา 36 มาตรา 37 และมาตรา 40 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
	เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชกำหนดนี้ เพื่อคุ้มครองประชาชนผู้สุจริตซึ่งถูกหลอกลวงจนสูญเสียไปซึ่งทรัพย์สิน โดยผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ซึ่งแต่ละวันมีผู้ถูกหลอกลวงจำนวนมากและมีมูลค่าความเสียหายสูงมาก สมควรมีมาตรการเพื่อป้องกันและปราบปรามอาชญากรรมประเภทนี้ให้หมดไปโดยเร็ว อันเป็นกรณีฉุกเฉินที่มีความจำเป็นรีบด่วนอันมิอาจจะหลีกเลี่ยงได้ เพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในทางเศรษฐกิจของประเทศ ซึ่งการตราพระราชกำหนดนี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย อาศัยอำนาจตามความในมาตรา 172 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชกำหนดขึ้นไว้ ดังต่อไปนี้ **มาตรา 1** พระราชกำหนดนี้เรียกว่า “พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568” **มาตรา 2** พระราชกำหนดนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
มาตรา 3 ในพระราชกำหนดนี้ “ผู้ประกอบธุรกิจ” หมายความว่า ผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงิน	**มาตรา 3** ให้ยกเลิกความในบทนิยามคำว่า “ผู้ประกอบธุรกิจ” ในมาตรา 3 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และให้ใช้ความต่อไปนี้แทน ““ผู้ประกอบธุรกิจ” หมายความว่า ผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงินและผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลตามกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล” **มาตรา 4** ให้เพิ่มความต่อไปนี้เป็นบทนิยามต่อจากบทนิยามคำว่า “ผู้ประกอบธุรกิจ” ในมาตรา 3 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ““กระเป๋าสินทรัพย์ดิจิทัล” หมายความว่า ระบบที่ใช้ในการจัดเก็บสินทรัพย์ดิจิทัล (wallet) “บัญชีเงินอิเล็กทรอนิกส์” หมายความรวมถึงบัญชีสินทรัพย์ดิจิทัล” **มาตรา 5** ให้ยกเลิกความในวรรคหนึ่งของมาตรา 4 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และให้ใช้ความต่อไปนี้แทน

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
มาตรา 4 เพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ในกรณีที่มีเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงินและผู้ประกอบธุรกิจมีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าที่เกี่ยวข้องในระหว่างสถาบันการเงินและผู้ประกอบธุรกิจนั้นผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน และธนาคารแห่งประเทศไทย เห็นชอบร่วมกัน	“มาตรา 4 เพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ในกรณีที่มีเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงินและผู้ประกอบธุรกิจมีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าที่เกี่ยวข้อง และเลขที่กระเป๋าสินทรัพย์ดิจิทัลในระหว่างสถาบันการเงินและผู้ประกอบธุรกิจนั้นผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน ธนาคารแห่งประเทศไทย และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ เห็นชอบร่วมกัน” **มาตรา 6** ให้เพิ่มความต่อไปนี้เป็นมาตรา 4/1 และมาตรา 4/2 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 “มาตรา 4/1 เพื่อประโยชน์แห่งมาตรา 8/10 ให้ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ และคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กำหนดมาตรฐานหรือมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยี

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
มาตรา 5 ในกรณีที่มีเหตุอันควรสงสัยว่ามีการกระทำความผิดอาชญากรรมทางเทคโนโลยีและมีความจำเป็นต้องทราบข้อมูลการลงทะเบียนผู้ใช้งานหรือข้อมูลจราจรทางคอมพิวเตอร์ ให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ	ให้ผู้ให้บริการเครือข่ายโทรศัพท์และผู้ให้บริการโทรคมนาคมอื่นมีหน้าที่ตรวจสอบเพื่อคัดกรองเนื้อหาการบริการสารสั้น (SMS) ที่อาจเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีตามมาตรฐานหรือมาตรการที่สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติกำหนดตามวรรคหนึ่ง มาตรา 4/2 เมื่อ ศปอท. ได้แจ้งรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยีตามประกาศในมาตรา 8/5 (6) ให้สถาบันการเงินหรือผู้ประกอบธุรกิจปฏิเสธการเปิดบัญชี ระงับการให้บริการหรือการทำธุรกรรม หรือปิดบัญชีกับบุคคลที่มีรายชื่อหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลดังกล่าว จนกว่าจะมีการเพิกถอนรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลนั้น” **มาตรา 7** ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา 5 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
หรือสำนักงานป้องกันและปราบปรามการฟอกเงิน แล้วแต่กรณี มีอำนาจสั่งให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องกับการกระทำดังกล่าว เปิดเผยข้อมูลที่เกี่ยวข้องเท่าที่จำเป็น และเมื่อได้รับคำสั่งแล้ว ให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องกับการกระทำนั้น มีหน้าที่ส่งข้อมูลดังกล่าวให้แก่ผู้สั่งภายในระยะเวลาที่ผู้สั่งกำหนด	“ในกรณีที่ปรากฏพยานหลักฐานอันควรเชื่อได้ว่ามีการใช้บริการโทรคมนาคมเพื่อกระทำความผิดอาชญากรรมทางเทคโนโลยีไม่ว่าจะปรากฏจากการตรวจสอบข้อมูลตามวรรคหนึ่งหรือพยานหลักฐานอื่นใด ให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน หรือ ศปอท. แล้วแต่กรณี แจ้งให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติสั่งให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องกับการกระทำนั้นระงับการให้บริการโทรคมนาคมดังกล่าว การยกเลิกการระงับการให้บริการตามวรรคสอง ให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ และ ศปอท. เห็นชอบร่วมกัน”

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
	มาตรา 8 ให้เพิ่มความต่อไปนี้เป็นมาตรา 7/1 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 “มาตรา 7/1 เมื่อความปรากฏต่อพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ว่ามีผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลโดยไม่ได้รับอนุญาตตามกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล ให้พนักงานเจ้าหน้าที่ดังกล่าวมีคำสั่งระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์หรือนำข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายออกจากระบบคอมพิวเตอร์โดยพลัน การสั่งระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์หรือนำข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายออกจากระบบคอมพิวเตอร์ตามวรรคหนึ่ง ให้ดำเนินการตามขั้นตอนที่รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมประกาศกำหนด” **มาตรา 9** ให้เพิ่มความต่อไปนี้เป็นมาตรา 8/1 มาตรา 8/2 มาตรา 8/3 มาตรา 8/4 มาตรา 8/5 มาตรา 8/6 มาตรา 8/7 มาตรา 8/8 มาตรา 8/9 มาตรา 8/10 มาตรา 8/11 และมาตรา 8/12 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
	“มาตรา 8/1 เพื่อประโยชน์ในการคืนเงินแก่ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี ให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ หรือสถาบันการเงินหรือผู้ประกอบธุรกิจรายงานข้อมูลเกี่ยวกับการทำธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ไปยังสำนักงานป้องกันและปราบปรามการฟอกเงิน ในการตรวจสอบรายงานตามวรรคหนึ่ง ให้เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินมอบหมายพนักงานเจ้าหน้าที่ตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินเป็นพนักงานเจ้าหน้าที่ผู้รับผิดชอบและอาจขอให้หน่วยงานของรัฐ สถาบันการเงินหรือผู้ประกอบธุรกิจที่เกี่ยวข้องให้ความช่วยเหลือ สนับสนุน หรือเข้าร่วมปฏิบัติหน้าที่ตามความเหมาะสมก็ได้ หน่วยงานของรัฐ สถาบันการเงินหรือผู้ประกอบธุรกิจตามวรรคสองต้องให้ความช่วยเหลือ สนับสนุน หรือมอบหมายบุคคลเข้าร่วมปฏิบัติหน้าที่ตามสมควรแก่กรณี และให้บุคคลที่ได้รับมอบหมายเข้าร่วมปฏิบัติหน้าที่ได้รับค่าตอบแทนตามระเบียบที่เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินกำหนดโดยได้รับความเห็นชอบของกระทรวงการคลัง การรายงานและการตรวจสอบรายงานให้เป็นไปตามหลักเกณฑ์วิธีการ เงื่อนไข และระยะเวลาที่กำหนดในกฎกระทรวง

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
	มาตรา 8/2 เมื่อสำนักงานป้องกันและปราบปรามการฟอกเงินได้ตรวจสอบรายงานตามมาตรา 8/1 แล้ว ให้ประกาศข้อมูลบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลซึ่งเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีในราชกิจจานุเบกษา และในประกาศดังกล่าว ให้แจ้งผู้เสียหายให้ยื่นคำร้องพร้อมแสดงหลักฐานแห่งความเสียหาย และแจ้งผู้ที่เกี่ยวข้องกับบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ ให้ยื่นคำร้องคัดค้านพร้อมแสดงหลักฐานว่าเงินในบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวไม่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ภายในเก้าสิบวันนับแต่วันที่ประกาศในราชกิจจานุเบกษา ในกรณีการแจ้งผู้เสียหายนั้น หากทราบตัวผู้เสียหายที่ชัดเจนแน่นอน ให้แจ้งให้ผู้เสียหายนั้นทราบโดยตรงอีกทางหนึ่งด้วย เมื่อพนักงานเจ้าหน้าที่ได้ตรวจสอบคำร้องตามวรรคหนึ่งแล้ว ให้พนักงานเจ้าหน้าที่เสนอเรื่องต่อคณะกรรมการธุรกรรมตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และให้คณะกรรมการธุรกรรมตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินมีอำนาจสั่งคืนเงินให้แก่ผู้เสียหาย การแจ้ง การยื่นคำร้อง การตรวจสอบคำร้อง การเสนอเรื่อง และการพิจารณาคืนเงินให้แก่ผู้เสียหาย การแจ้งผลการพิจารณาต่อผู้เสียหายและผู้ที่เกี่ยวข้อง และวิธีการคืนเงินให้แก่ผู้เสียหาย ให้เป็นไปตามหลักเกณฑ์ วิธีการ เงื่อนไข และระยะเวลาที่กำหนดในกฎกระทรวง

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
	ในกรณีที่ผู้เสียหายหรือผู้ที่เกี่ยวข้องไม่เห็นด้วยกับคำสั่งของคณะกรรมการธุรกรรมตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ให้ยื่นคำร้องต่อศาลแพ่งภายในสามสิบวันนับแต่วันที่ได้รับแจ้งผลการพิจารณา และให้นำหมวด 6 การดำเนินการเกี่ยวกับทรัพย์สินแห่งพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาใช้บังคับโดยอนุโลม คำพิพากษาของศาลอุทธรณ์ให้เป็นที่สุด มาตรา 8/3 ให้นำมาตรา 8/1 และมาตรา 8/2 มาใช้บังคับแก่กรณีที่สำนักงานป้องกันและปราบปรามการฟอกเงินพบเหตุอันควรสงสัยเองหรือได้รับข้อมูลจากระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา 4 ด้วยโดยอนุโลม มาตรา 8/4 ในกรณีปรากฏข้อเท็จจริงว่าบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ใด ไม่มีผู้เสียหายหรือผู้ที่เกี่ยวข้องมายื่นคำร้องภายในสิบปีนับแต่วันที่ครบกำหนดตามมาตรา 8/2 หรือปรากฏข้อเท็จจริงว่าได้คืนเงินให้แก่ผู้เสียหายแล้วแต่ยังมีเงินเหลืออยู่ในบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ ให้เงินในบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวตกเป็นของกองทุนป้องกันและปราบปรามการฟอกเงิน แต่ไม่ตัดสิทธิเจ้าของเงินหรือเจ้าของบัญชีที่จะขอรับเงินคืนจากกองทุนป้องกันและปราบปรามการฟอกเงินภายหลังจากนั้น ถ้าพิสูจน์ได้ว่าตนมีเหตุอันสมควรที่ไม่อาจมารับคืนได้ภายในกำหนดเวลาดังกล่าว ในกรณีเช่นนั้น ให้คืนเงินให้แก่ผู้นั้น

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
	มาตรา 8/5 ให้จัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เรียกโดยย่อว่า “ศปอท.” ในสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีหน้าที่และอำนาจดังต่อไปนี้ (1) รับแจ้งเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยีจากผู้เสียหาย และให้ถือว่าการแจ้งเหตุดังกล่าวเป็นการร้องทุกข์โดยวิธีการทางอิเล็กทรอนิกส์ตามมาตรา 8 วรรคสอง (2) ระงับการทำธุรกรรมที่เป็นบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ที่ปรากฏพยานหลักฐานอันควรเชื่อได้ว่าเกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยีโดยทันที หรือเพิกถอนการระงับการทำธุรกรรมดังกล่าวในกรณีที่พิสูจน์ได้ว่ามิได้เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี (3) สั่งให้สถาบันการเงินหรือผู้ประกอบธุรกิจนำส่งข้อมูลเกี่ยวกับบัญชีและธุรกรรมที่ต้องสงสัย (4) รวบรวมจำนวนบัญชีเงินฝากที่บุคคลใดถือไว้ เพื่อประโยชน์ในการตรวจสอบว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยี แต่ทั้งนี้ ไม่รวมถึงจำนวนเงินฝากทั้งหมดหรือของแต่ละบัญชี

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
	(5) เปิดเผยหรือแลกเปลี่ยนข้อมูลที่เกี่ยวข้องเพื่อประโยชน์ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีกับหน่วยงานของรัฐและหน่วยงานเอกชนที่เกี่ยวข้อง (6) ประกาศรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี และเพิกถอนรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลดังกล่าว ทั้งนี้ ตามหลักเกณฑ์ที่ ศปอท. ประกาศกำหนด (7) แจ้งข้อมูลหมายเลขโทรศัพท์ บริการสารสั้น (SMS) หรือชื่อผู้ส่งสารสั้นหรือข้อมูลการใช้บริการโทรคมนาคมอื่น ให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติทราบเพื่อดำเนินการตามมาตรา 5 วรรคสอง (8) รวบรวมข้อมูลเกี่ยวกับอาชญากรรมทางเทคโนโลยีเพื่อปฏิบัติการตามพระราชกำหนดนี้ (9) จัดทำรายงานผลการดำเนินการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเสนอคณะกรรมการตามมาตรา 13 เดือนละหนึ่งครั้ง มาตรา 8/6 ให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงาน

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
	คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือหน่วยงานอื่นของรัฐหรือหน่วยงานของเอกชนที่รัฐมนตรีประกาศกำหนด แต่งตั้งผู้แทนเข้าร่วมปฏิบัติงานใน ศปอท. มาตรา 8/7 ให้คณะกรรมการตามมาตรา 13 แต่งตั้งหัวหน้า ศปอท. โดยมีหน้าที่และอำนาจดังต่อไปนี้ (1) รับผิดชอบในการบริหารงานของ ศปอท. (2) เป็นผู้แทนของ ศปอท. ในการติดต่อกับบุคคลภายนอก (3) ปฏิบัติหน้าที่อื่นตามที่กำหนดไว้ในพระราชกำหนดนี้ (4) ปฏิบัติการอื่นตามที่คณะกรรมการตามมาตรา 13 มอบหมาย มาตรา 8/8 รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อาจวางระเบียบการปฏิบัติงานของ ศปอท. ก็ได้ มาตรา 8/9 ให้เจ้าหน้าที่ซึ่งได้รับการแต่งตั้งให้ปฏิบัติงานใน ศปอท. ได้รับค่าตอบแทนตามระเบียบที่รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมประกาศกำหนดโดยความเห็นชอบของกระทรวงการคลัง มาตรา 8/10 ให้สถาบันการเงินหรือผู้ประกอบธุรกิจ ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น ผู้ให้บริการอื่นที่เกี่ยวข้อง หรือผู้ให้บริการสื่อสังคมออนไลน์ มีส่วนร่วมรับผิดชอบในความเสียหายที่เกิดจากอาชญากรรมทางเทคโนโลยี เว้นแต่จะพิสูจน์ได้ว่าสถาบันการเงินหรือผู้ประกอบธุรกิจ

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
	ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น ผู้ให้บริการอื่นที่เกี่ยวข้อง หรือผู้ให้บริการสื่อสังคมออนไลน์ ได้ปฏิบัติตามมาตรฐานหรือมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีที่กำหนดโดยธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ แล้วแต่กรณี มาตรา 8/11 สถาบันการเงินหรือผู้ประกอบธุรกิจใดไม่ปฏิบัติตามมาตรา 4/2 ต้องระวางโทษปรับไม่เกินห้าแสนบาท ในกรณีที่การกระทำความผิดตามวรรคหนึ่งเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ มาตรา 8/12 ผู้ใดไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ตามมาตรา 7/1 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
	มาตรา 10 ให้เพิ่มความต่อไปนี้เป็นมาตรา 11/1 และมาตรา 11/2 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 “มาตรา 11/1 ในกรณีที่ผู้ซื้อเลขหมายโทรศัพท์ลงทะเบียนเพื่อใช้บริการหรือผู้ขายเลขหมายโทรศัพท์ที่มีหน้าที่เกี่ยวกับการลงทะเบียนให้แก่ผู้ใช้บริการลงทะเบียนไม่ถูกต้องครบถ้วนตามที่คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติกำหนด โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ มาตรา 11/2 ผู้ใดใช้ข้อมูลเกี่ยวกับบุคคลหรือผู้ถึงแก่กรรมซึ่งทำให้สามารถระบุตัวบุคคลหรือผู้ถึงแก่กรรมนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เพื่อกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ ผู้ใดเก็บรวบรวม ครอบครอง หรือเปิดเผยข้อมูลเกี่ยวกับบุคคลหรือผู้ถึงแก่กรรมซึ่งทำให้สามารถระบุตัวบุคคลหรือผู้ถึงแก่กรรมนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เพื่อนำไปใช้หรือให้บุคคลอื่นใช้ในการกระทำความผิดเกี่ยวกับ

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี พ.ศ. 2566	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 (คณะรัฐมนตรี เป็นผู้เสนอ)
	อาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษตามที่บัญญัติในวรรคหนึ่ง ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสองได้กระทำโดยซื้อ เสนอซื้อ ขาย เสนอขาย แลกเปลี่ยน เสนอแลกเปลี่ยน หรือแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ”

ส่วนที่ 2
บทวิเคราะห์

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 ได้มีการปรับปรุงและเพิ่มเติมหลายมาตรา เพื่อตอบสนองต่อภัยคุกคามทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว โดยมีเป้าหมายหลักในการยับยั้งเส้นทางการกระทำผิด ลดความเสียหายแก่ประชาชน และเพิ่มประสิทธิภาพในการติดตาม ตรวจสอบ และลงโทษผู้กระทำความผิด โดยพระราชกำหนดดังกล่าวมีสาระสำคัญ ดังนี้

1. การนำเงินที่ได้จากอาชญากรรมทางเทคโนโลยีไปซื้อขายสินทรัพย์ดิจิทัล

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 ได้กำหนดแนวทางทางกฎหมายไว้หลายประการเพื่อยกระดับประสิทธิภาพในการควบคุม ป้องกัน และแก้ไขปัญหาการฟอกเงินผ่านสินทรัพย์ดิจิทัลที่ทำให้ยากต่อการตรวจสอบและระงับธุรกรรม โดยมุ่งเน้นการปิดช่องว่างทางกฎหมายที่อาชญากรใช้ในการเคลื่อนย้ายเงินผิดกฎหมายเข้าสู่ระบบสินทรัพย์ดิจิทัล และเสริมสร้างอำนาจให้กับหน่วยงานรัฐในการติดตาม ตรวจสอบ ยึดคืน และคืนทรัพย์ให้แก่ผู้เสียหายได้อย่างเป็นธรรมและทันท่วงที โดยมีหลักกฎหมายที่เกี่ยวข้อง สรุปได้ดังนี้

1.1 แก้ไขคำจำกัดความ “ผู้ประกอบธุรกิจ” การกำหนดความหมายของ “ผู้ประกอบธุรกิจ” ให้รวมถึงผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงินและผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลตามกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล การแก้ไขดังกล่าวมีผลโดยตรงต่อการควบคุมและตรวจสอบธุรกรรมทางการเงินที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล ซึ่งเป็นแนวทางที่มีศักยภาพในการยกระดับการควบคุมธุรกรรมทางการเงิน โดยเฉพาะธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี เช่น การฟอกเงินผ่านสินทรัพย์ดิจิทัลหรือการนำเงินที่ได้จากอาชญากรรมไปซื้อขายคริปโทเคอร์เรนซี การขยายขอบเขตนิยามนี้เปิดโอกาสให้ภาครัฐสามารถบังคับใช้มาตรการตรวจสอบและป้องกันที่เข้มงวดมากขึ้น โดยกำหนดให้ธุรกิจประเภทนี้ต้องปฏิบัติตามหลักเกณฑ์การยืนยันตัวตนผู้ใช้งาน (Know Your Customer: KYC) และการป้องกันการฟอกเงิน (Anti-Money Laundering: AML) อย่างเคร่งครัด ส่งผลให้หน่วยงานรัฐสามารถติดตามเส้นทางการเงินโดยการย้อนกลับไปยังต้นตอของเงินที่ได้จากการกระทำความผิดและดำเนินคดีได้อย่างมีประสิทธิภาพ

การกำหนดให้การดำเนินธุรกิจสินทรัพย์ดิจิทัลอยู่ภายใต้การควบคุมของกฎหมายยังคงถือเป็นกลไกสำคัญในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยเฉพาะในยุคที่การใช้สินทรัพย์ดิจิทัลเพิ่มขึ้นอย่างรวดเร็วและข้ามพรมแดนได้โดยง่าย

1.2 เพิ่มนิยาม “กระเป๋าสินทรัพย์ดิจิทัล” และ “บัญชีเงินอิเล็กทรอนิกส์” กระเป๋าสินทรัพย์ดิจิทัลและบัญชีเงินอิเล็กทรอนิกส์เป็นเครื่องมือที่ถูกใช้ในการแปลงและเคลื่อนย้ายเงินจากอาชญากรรมทางเทคโนโลยีสู่กระเป๋าสินทรัพย์ดิจิทัลและบัญชีเงินอิเล็กทรอนิกส์ เช่น การหลอกลวงออนไลน์หรือโจรกรรมข้อมูล โดยผู้กระทำผิดมักโอนเงินไปยังกระเป๋าสินทรัพย์ดิจิทัลหรือบัญชีที่ไม่ระบุตัวตน ทำให้ยากต่อการตรวจสอบที่มาของเงินและการระงับธุรกรรม เนื่องจากบางระบบไม่อยู่ภายใต้การกำกับของรัฐ อีกทั้งยังสามารถถ่ายโอนเงินข้ามแพลตฟอร์มได้อย่างรวดเร็ว การควบคุมกระเป๋าและบัญชีเหล่านี้จึงควรอยู่ภายใต้กฎหมายที่ชัดเจน

มีการยืนยันตัวตนผู้ใช้งาน (KYC) และมาตรการป้องกันการฟอกเงิน (AML) ที่เข้มงวด เพื่อให้รัฐสามารถตรวจสอบธุรกรรมต้องสงสัยและดำเนินการอายัดทรัพย์สินได้อย่างทันท่วงที ซึ่งจะช่วยลดช่องโหว่ในการฟอกเงินผ่านสินทรัพย์ดิจิทัลและยกระดับประสิทธิภาพในการปราบปรามอาชญากรรมทางเทคโนโลยีในภาพรวม

1.3 มาตรา 4/2 ได้วางหลักให้สถาบันการเงินหรือผู้ประกอบธุรกิจระงับหรือปิดบัญชีที่เกี่ยวข้องกับกระเป๋าสินทรัพย์ดิจิทัล เมื่อได้รับการแจ้งรายชื่อบุคคลหรือเลขที่กระเป๋าดิจิทัลที่เกี่ยวกับการกระทำอาชญากรรมทางเทคโนโลยีตามประกาศ ศปอท. ถือได้ว่าเป็นมาตรการเชิงรุกที่ช่วยสกัดการฟอกเงินผ่านสินทรัพย์ดิจิทัล ซึ่งมักมีลักษณะไร้ตัวตนและโอนย้ายข้ามแพลตฟอร์มได้รวดเร็วทำให้ยากต่อการติดตาม หากไม่ดำเนินการอย่างทันท่วงทีอาชญากรสามารถซ่อนหรือเคลื่อนย้ายทรัพย์สินได้ นอกจากนี้ การให้สิทธิแก่รัฐในการสั่งระงับหรือปิดบัญชีโดยไม่ต้องรอคำสั่งศาลจะช่วยลดช่องว่างในการดำเนินคดีและเพิ่มโอกาสในการติดตามและยึดคืนทรัพย์สินกลับคืนสู่ผู้เสียหายหรือรัฐได้อย่างมีประสิทธิภาพยิ่งขึ้น

1.4 มาตรา 7/1 วางหลักเกี่ยวกับการระงับการเผยแพร่ข้อมูลหรือปิดเว็บที่ให้บริการสินทรัพย์ดิจิทัลโดยไม่ได้รับอนุญาต ซึ่งให้อำนาจพนักงานเจ้าหน้าที่ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในการสั่งระงับหรือถอดถอนข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่ไม่ได้รับอนุญาต ซึ่งเป็นกลไกสำคัญในการป้องกันและสกัดกั้นการฟอกเงินผ่านแพลตฟอร์มที่ผิดกฎหมาย โดยเฉพาะกรณีที่ผู้กระทำความผิดใช้เว็บไซต์หรือแอปพลิเคชันที่ไม่อยู่ภายใต้การกำกับของรัฐในการซื้อขายหรือโอนย้ายสินทรัพย์ดิจิทัล ซึ่งการระงับการเผยแพร่ข้อมูลและการถอดถอนเนื้อหาออกจากระบบอย่างรวดเร็ว ทำให้ช่วยยับยั้งการเข้าถึงของประชาชนและจำกัดการเคลื่อนไหวของอาชญากรในโลกดิจิทัลได้ทันเวลา ลดความเสี่ยงในการนำเงินจากอาชญากรรมเข้าสู่ระบบสินทรัพย์ดิจิทัล และเสริมความเข้มแข็งในการควบคุมธุรกรรมที่ผิดกฎหมายในยุคดิจิทัลอย่างมีประสิทธิภาพ

1.5 มาตรา 8/10 กำหนดให้ผู้ให้บริการที่เกี่ยวข้องมีความรับผิดร่วม โดยได้วางหลักให้สถาบันการเงิน ผู้ให้บริการโทรคมนาคม และผู้ให้บริการสื่อสังคมออนไลน์ต้องมีส่วนร่วมรับผิดชอบ หากละเลยหรือไม่ปฏิบัติตามมาตรฐานที่กำหนดไว้ ซึ่งหลักกฎหมายดังกล่าว มีเป้าหมายสร้างแรงจูงใจให้สถาบันการเงิน ผู้ให้บริการโทรคมนาคม และแพลตฟอร์มออนไลน์ต่าง ๆ มีส่วนร่วมในการป้องกันอาชญากรรมทางเทคโนโลยี โดยกำหนดให้ต้องร่วมรับผิดชอบต่อความเสียหายที่เกิดขึ้น เว้นแต่สามารถพิสูจน์ได้ว่าได้ปฏิบัติตามมาตรการหรือมาตรฐานที่หน่วยงานกำกับดูแลกำหนดไว้แล้ว ซึ่งส่งผลให้ผู้ให้บริการดังกล่าวต้องยกระดับระบบตรวจสอบธุรกรรม ยืนยันตัวตนผู้ใช้งาน (KYC) และกลไกการแจ้งเตือนธุรกรรมผิดปกติให้เข้มงวดยิ่งขึ้น การเพิ่มความรับผิดชอบในระดับต้นทางนี้ช่วยลดช่องว่างที่มิจฉาชีพใช้ในการโอนเงินผิดกฎหมายเข้าสู่ระบบสินทรัพย์ดิจิทัล ชะลอหรือสกัดกระบวนการฟอกเงินที่ยากต่อการติดตามในภายหลัง และเสริมให้ทุกภาคส่วนมีบทบาทร่วมกันในการป้องกันและลดผลกระทบจากอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพยิ่งขึ้น

1.6 มาตรา 8/11 กำหนดโทษในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจไม่ปฏิบัติตามคำสั่งระงับบัญชีเป็นกลไกสำคัญในการสร้างความรับผิดชอบแก่สถาบันการเงินและผู้ประกอบธุรกิจที่ละเลยต่อหน้าที่ในการป้องกันอาชญากรรมทางเทคโนโลยี โดยกำหนดโทษปรับกรณีองค์กรไม่ปฏิบัติตาม และโทษจำคุกหรือปรับแก่กรรมการหรือผู้บริหารที่มีส่วนเกี่ยวข้องโดยตรงหรือโดยละเลย ซึ่งช่วยกระตุ้นให้หน่วยงานปฏิบัติตาม

มาตรฐานป้องกันความเสี่ยง เช่น การตรวจสอบธุรกรรมต้องสงสัย การยืนยันตัวตนผู้ใช้งาน และการแจ้งเตือนธุรกรรมผิดปกติอย่างเคร่งครัด ทำให้ลดโอกาสที่อาชญากรจะใช้ระบบการเงินในการฟอกเงินผ่านสินทรัพย์ดิจิทัลที่ติดตามได้ยาก มาตรการลงโทษนี้เป็นส่วนสำคัญที่ทำให้ทุกฝ่ายต้องร่วมมือกันปิดช่องว่างและสกัดกระบวนการฟอกเงินได้อย่างมีประสิทธิภาพ

2. การใช้บริการโทรคมนาคมในการกระทำความผิด

การแก้ไขเพิ่มเติมกฎหมายในส่วนที่เกี่ยวข้องกับการใช้บริการโทรคมนาคมในการกระทำความผิดทางเทคโนโลยี แสดงให้เห็นถึงความมุ่งมั่นในการแก้ไขปัญหาอาชญากรรมทางอิเล็กทรอนิกส์ที่นับวันจะมีความรุนแรงและซับซ้อนมากยิ่งขึ้น โดยมีบริการโทรคมนาคมเป็นช่องทางสำคัญที่ถูกนำมาใช้ในการก่อเหตุ โดยมีหลักกฎหมายที่เกี่ยวข้อง สรุปได้ดังนี้

2.1 การกระทำผิดหลายกรณีอาศัยบริการโทรศัพท์หรืออินเทอร์เน็ตเป็นช่องทางในการกระทำความผิด จึงมีการเพิ่มมาตรา 4/1 และมาตรา 5 วรรคสองและสาม กำหนดให้ผู้ให้บริการเครือข่ายต้องมีหน้าที่ตรวจสอบและคัดกรองเนื้อหาการบริการข้อความสั้น (SMS) และการเพิ่มบทบัญญัติเกี่ยวกับการระงับการให้บริการโทรคมนาคมที่ใช้ในการกระทำผิดอาชญากรรมทางเทคโนโลยี จะสามารถช่วยเพิ่มประสิทธิภาพในการติดตามเส้นทางการเงินของผู้กระทำผิดได้อย่างรวดเร็ว ลดโอกาสที่เงินจากการกระทำผิดจะถูกเคลื่อนย้ายหรือฟอกเงินผ่านระบบสินทรัพย์ดิจิทัลที่มีลักษณะกระจายตัวและตรวจสอบได้ยาก นอกจากนี้ การให้อำนาจระงับบริการโทรคมนาคมที่เกี่ยวข้องกับการกระทำผิดทันทียังเป็นมาตรการสำคัญในการสกัดกั้นการกระทำความผิดตั้งแต่ต้นทาง ลดโอกาสที่ผู้กระทำผิดจะใช้ช่องทางการสื่อสารเพื่อหลอกลวงหรือก่ออาชญากรรมต่อเนื่องได้

2.2 มาตรา 8/10 ให้สถาบันการเงิน ผู้ประกอบธุรกิจ ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคม ผู้ให้บริการแพลตฟอร์มดิจิทัล และสื่อสังคมออนไลน์ที่เกี่ยวข้อง ซึ่งระบบหรือบริการของตนถูกนำไปใช้กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี มีหน้าที่ร่วมรับผิดชอบต่อความเสียหายที่เกิดขึ้น เว้นแต่จะพิสูจน์ได้ว่าตนได้ดำเนินการตามมาตรฐานหรือมาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์และการป้องกันอาชญากรรมทางเทคโนโลยี ตามที่ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือคณะกรรมการธุรกรรมอิเล็กทรอนิกส์กำหนดไว้ แล้วแต่กรณี

2.3 มาตรา 11/1 ได้วางหลักเพื่อควบคุมและป้องกันการใช้เลขหมายโทรศัพท์เป็นเครื่องมือในการกระทำความผิดทางเทคโนโลยี โดยเฉพาะการใช้เลขหมายโทรศัพท์ที่ลงทะเบียนโดยไม่ถูกต้อง หรือใช้บุคคลอื่นในการลงทะเบียนเพื่อปกปิดตัวตนของมิจฉาชีพ ซึ่งเป็นพฤติกรรมที่มิจฉาชีพมักใช้เพื่อก่ออาชญากรรม เช่น การโทรหลอกลวง ส่ง SMS ปลอม เป็นต้น เพื่อเข้าถึงบัญชีของผู้อื่น กฎหมายจึงกำหนดบทลงโทษแก่ผู้ซื้อและผู้ขายเลขหมายโทรศัพท์ที่ละเลยต่อการลงทะเบียนให้ถูกต้องครบถ้วน โดยที่รู้หรือควรรู้ว่าเลขหมายดังกล่าวจะถูกนำไปใช้ในการกระทำความผิด บทลงโทษทางอาญาที่กำหนดไว้จะทำให้ผู้เกี่ยวข้องกับการลงทะเบียนมีความระมัดระวังมากขึ้น และไม่เอื้อประโยชน์ให้กับมิจฉาชีพ อีกทั้งยังเป็นการสร้างกลไกบังคับใช้กฎหมายที่เชื่อมโยงกับการควบคุมต้นทางของปัญหา กล่าวคือ หากสามารถควบคุมการลงทะเบียนเลขหมายโทรศัพท์

ได้อย่างรัดกุม ก็จะช่วยลดจำนวนเลขหมายโทรศัพท์ที่มิจฉาชีพใช้ในการก่อเหตุและเพิ่มประสิทธิภาพในการติดตามตัวผู้กระทำผิดผ่านข้อมูลการลงทะเบียนที่ถูกต้อง จึงถือเป็นมาตรการสำคัญในการตัดวงจรการใช้บริการโทรคมนาคมในการกระทำความผิดทางเทคโนโลยี

3. ปัญหาความล่าช้าในการคืนเงินให้ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี

ผู้เสียหายจากอาชญากรรมทางเทคโนโลยีส่วนใหญ่มักไม่สามารถติดตามและนำเงินที่ถูกหลอกลวงไปกลับคืนมาได้ เนื่องจากความซับซ้อนของระบบการไหลเวียนเงินในธุรกรรมดิจิทัล ทำให้การติดตามเส้นทางการเงินเป็นไปได้ยาก มาตรา 8/1 - 8/4 จึงได้วางหลักการรายงาน ตรวจสอบ ประกาศ และคืนเงินให้ผู้เสียหายอย่างเป็นระบบ ดังนี้

3.1 การรายงานข้อมูลธุรกรรมที่น่าสงสัยและความร่วมมือระหว่างหน่วยงาน

กำหนดให้สถาบันการเงินรายงานข้อมูลธุรกรรมที่น่าสงสัยไปยังสำนักงานป้องกันและปราบปรามการฟอกเงิน (สำนักงาน ปปง.) และให้อำนาจเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินในการแต่งตั้งพนักงานเจ้าหน้าที่ตรวจสอบ พร้อมทั้งกำหนดให้หน่วยงานรัฐและเอกชนที่เกี่ยวข้องต้องให้ความร่วมมือ โดยมีค่าตอบแทนที่ชัดเจนเพื่อส่งเสริมการทำงานร่วมกัน ซึ่งจะช่วยลดอุปสรรคในการดำเนินงานร่วมกันของภาครัฐและเอกชน

3.2 ขั้นตอนการคืนเงิน

กำหนดขั้นตอนการคืนเงิน เริ่มตั้งแต่การประกาศข้อมูลบัญชีของบุคคลซึ่งเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี การแจ้งผู้เสียหายให้ยื่นคำร้อง การตรวจสอบข้อเท็จจริง และการให้อำนาจคณะกรรมการธุรกรรมในการสั่งคืนเงิน รวมถึงเปิดโอกาสให้ผู้เสียหายหรือผู้ที่เกี่ยวข้องสามารถอุทธรณ์ต่อศาลได้เพื่อคุ้มครองสิทธิของทุกฝ่าย

3.3 การให้อำนาจสำนักงานป้องกันและปราบปรามการฟอกเงิน ในกรณีพบเหตุอันควรสงสัย

อนุญาตให้สำนักงานป้องกันและปราบปรามการฟอกเงิน (สำนักงาน ปปง.) สามารถดำเนินการตรวจสอบและคืนเงินได้ในกรณีที่พบเหตุอันควรสงสัยหรือได้รับข้อมูลจากกระบวนการการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา 4 แม้จะไม่มีรายงานจากตำรวจหรือสถาบันการเงินโดยตรง ซึ่งเป็นการเพิ่มความคล่องตัวในการรับมือกับอาชญากรรมทางเทคโนโลยี

3.4 การจัดการทรัพย์สินที่ไม่มีผู้มาแสดงสิทธิ

กำหนดแนวทางการจัดการทรัพย์สินที่ไม่มีผู้มาแสดงสิทธิ หรือทรัพย์สินที่เหลือจากการคืนเงินโดยนำเข้าสู่กองทุนเพื่อใช้ในภารกิจป้องกันการฟอกเงิน แต่ยังคงเปิดโอกาสให้เจ้าของทรัพย์สินสามารถพิสูจน์และขอคืนได้ในภายหลัง ซึ่งเป็นการสร้างความสมดุลระหว่างประโยชน์สาธารณะและสิทธิส่วนบุคคล

ดังนั้น พระราชกำหนดฉบับนี้จึงมีเป้าหมายเพื่อสร้างระบบการติดตาม ตรวจสอบ และคืนทรัพย์สินแก่ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี โดยอาศัยความร่วมมือจากทุกภาคส่วน และให้ความสำคัญกับการคุ้มครองสิทธิของผู้เสียหายและผู้ที่เกี่ยวข้องอย่างเป็นธรรม

4. การระงับการทำให้แพร่หลายหรือการนำข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายออกจากระบบในกรณีการประกอบธุรกิจสินทรัพย์ดิจิทัลโดยไม่ได้รับอนุญาต

เพื่อป้องกันการประกอบธุรกิจผิดกฎหมาย โดยเฉพาะในกรณีของธุรกิจสินทรัพย์ดิจิทัลที่ไม่ได้รับอนุญาต ซึ่งมักถูกใช้เป็นช่องทางในการฉ้อโกงหรือฟอกเงิน จึงมีการเพิ่ม มาตรา 7/1 ที่วางหลักให้ พนักงานเจ้าหน้าที่มีอำนาจสั่งระงับการเผยแพร่ข้อมูลหรือสั่งให้นำข้อมูลที่ผิดกฎหมายออกจากระบบคอมพิวเตอร์ในกรณีที่มีการประกอบธุรกิจสินทรัพย์ดิจิทัลโดยไม่ได้รับอนุญาตได้ทันที ซึ่งมาตรการนี้มีเป้าหมายเพื่อจัดการกับการหลอกลวงประชาชนผ่านแพลตฟอร์มที่ไม่อยู่ภายใต้การควบคุมของกฎหมาย เช่น การชักชวนลงทุนในรูปแบบผิดกฎหมายผ่านสื่อออนไลน์ เป็นต้น

หลักกฎหมายดังกล่าวข้างต้น ทำให้เจ้าหน้าที่สามารถดำเนินการหยุดยั้งการเผยแพร่ข้อมูลผิดกฎหมายได้อย่างรวดเร็ว ลดโอกาสที่ประชาชนจะตกเป็นเหยื่อของการหลอกลวงสามารถควบคุมความเสียหายตั้งแต่ระยะเริ่มต้นก่อนที่ผลกระทบจะลุกลาม ทั้งนี้ หลักกฎหมายดังกล่าวเป็นเครื่องมือสำคัญที่ช่วยให้ภาครัฐสามารถรับมือกับภัยคุกคามทางเทคโนโลยีและอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากขึ้น

5. การจัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเพื่อประสานงานและแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี

มาตรา 8/5 ถึง 8/9 ของพระราชกำหนดฉบับนี้ได้กำหนดให้มีการจัดตั้ง “ศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี” หรือ “ศปอท.” ขึ้นในสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งนับว่าเป็นกลไกเชิงรุกที่มุ่งเน้นการตอบสนองต่อภัยคุกคามจากอาชญากรรมทางเทคโนโลยีอย่างรวดเร็วและมีประสิทธิภาพ โดยการกำหนดอำนาจหน้าที่ที่ครอบคลุมทั้งการรับแจ้งเหตุ การระงับธุรกรรมที่ต้องสงสัย การรวบรวมข้อมูล การแลกเปลี่ยนข่าวสารกับหน่วยงานต่าง ๆ และการเปิดเผยข้อมูลสู่สาธารณะ ถือเป็นการสร้างกลไกกลางที่เชื่อมโยงข้อมูลและปฏิบัติการจากหลายภาคส่วนทั้งภาครัฐและเอกชนอย่างเป็นระบบ นอกจากนี้ยังมีบทบัญญัติรองรับการแต่งตั้งบุคลากรจากหน่วยงานหลัก เช่น สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เพื่อเสริมความเชี่ยวชาญเฉพาะด้าน ส่งผลให้การสืบสวน การระงับความเสียหาย และการแจ้งเตือนภัยมีความครบถ้วนและรวดเร็ว รวมทั้งการให้หัวหน้า ศปอท. มีอำนาจในการบริหารงานและเป็นตัวแทนในการประสานงานกับหน่วยงานภายนอก ช่วยให้เกิดการตอบสนองที่ดีขึ้น ขณะที่การกำหนดให้มีรายงานผลการดำเนินงานต่อคณะกรรมการตามที่กฎหมายกำหนดเดือนละ 1 ครั้ง ช่วยเพิ่มความโปร่งใสและความรับผิดชอบในการดำเนินงาน รวมไปถึงการที่รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมสามารถวางระเบียบเพิ่มเติมและกำหนดค่าตอบแทนแก่เจ้าหน้าที่ยังเป็นแรงจูงใจในการดึงดูดบุคลากรที่มีความสามารถเข้าสู่ระบบ สะท้อนให้เห็นว่าหลักกฎหมายดังกล่าววางรากฐานเพื่อสร้างระบบที่มีประสิทธิภาพต่อการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีอย่างยั่งยืน

6. ความรับผิดของผู้ประกอบธุรกิจ

เพื่อป้องกันและลดความเสี่ยงจากอาชญากรรมทางเทคโนโลยี รวมถึงกระตุ้นให้ผู้ประกอบธุรกิจดำเนินมาตรการอย่างจริงจัง กฎหมายฉบับนี้ได้เพิ่ม มาตรา 8/10 วางหลักให้ ผู้ประกอบธุรกิจที่ละเลยมาตรการป้องกัน ต้องร่วมรับผิดชอบชดใช้ความเสียหายแก่ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี เนื่องจากผู้เสียหายส่วนใหญ่มักไม่สามารถติดตามทรัพย์สินคืนได้ทันเวลา อีกทั้งยังพบว่าระบบของสถาบันการเงิน ผู้ให้บริการโทรคมนาคม หรือ แพลตฟอร์มสื่อสังคมออนไลน์บางรายมีข้อบกพร่อง เช่น ระบบยืนยันตัวตนที่หละหลวม การเปิดบัญชีโดยไม่ตรวจสอบข้อมูลลูกค้าอย่างรัดกุม การให้บริการที่ไม่สามารถติดตามตัวผู้กระทำผิดได้ การตั้งค่าความปลอดภัยไม่เพียงพอ ขาดระบบแจ้งเตือนหรือปิดกั้นธุรกรรมผิดปกติได้ทันเวลา เป็นต้น ข้อบกพร่องเหล่านี้เป็นช่องว่างที่ทำให้มิจฉาชีพสามารถแอบอ้างตัวตนของผู้ใช้บริการในการกระทำความผิด ส่งผลให้ความเสียหายขยายวงกว้างและการติดตามทรัพย์หรือผู้กระทำผิดทำได้ล่าช้า ด้วยเหตุนี้ ผู้ประกอบธุรกิจ เช่น ธนาคาร ผู้ประกอบธุรกิจโทรคมนาคม หรือแพลตฟอร์มออนไลน์ ต้องมีส่วนร่วมรับผิดชอบในความเสียหายที่เกิดขึ้นยกเว้นจะพิสูจน์ได้ว่าได้ปฏิบัติตามมาตรฐานที่กำหนดไว้โดยหน่วยงานกำกับ เช่น ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เป็นต้น

ทั้งนี้ แนวทางดังกล่าวจะช่วยผลักดันให้ผู้ประกอบธุรกิจปรับปรุงระบบรักษาความปลอดภัยอย่างจริงจัง และทำให้ผู้เสียหายได้รับการเยียวยาได้รวดเร็วขึ้น ลดภาระการติดตามทรัพย์ด้วยตนเอง อย่างไรก็ตาม แนวทางดังกล่าวนี้ยังมีประเด็นที่ต้องพิจารณา คือ ภาระความรับผิดที่อาจทำให้ต้นทุนผู้ประกอบธุรกิจเพิ่มขึ้น และส่งผลต่อต้นทุนบริการหรือการเข้าถึงของประชาชน ดังนั้น การกำหนดมาตรการนี้ควรมีมาตรฐานกลางที่ชัดเจน โปร่งใส และสอดคล้องกับลักษณะธุรกิจแต่ละประเภท เปิดช่องให้ผู้ประกอบธุรกิจสามารถพิสูจน์การปฏิบัติตามมาตรฐานได้อย่างยุติธรรมเพื่อให้เกิดความสมดุลระหว่างการคุ้มครองผู้บริโภค และความมั่นคงในการดำเนินธุรกิจของผู้ประกอบธุรกิจต่อไป

7. การนำข้อมูลของบุคคลหรือผู้ถึงแก่กรรมมาใช้ในการกระทำความผิด

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 ได้เพิ่มมาตรา 11/2 เพื่อรับมือกับปัญหาการนำข้อมูลของบุคคล หรือข้อมูลของผู้ที่เสียชีวิตไปใช้ในการกระทำความผิด โดยเฉพาะในรูปแบบของอาชญากรรมทางเทคโนโลยี เช่น การปลอมตัว การเปิดบัญชีม้า หรือการหลอกลวงผ่านแพลตฟอร์มออนไลน์ สาระสำคัญของมาตรานี้ คือ กำหนดให้ผู้ใดที่ใช้ เก็บรวบรวม ครอบครอง หรือเปิดเผยข้อมูลเกี่ยวกับบุคคล หรือข้อมูลของผู้ถึงแก่กรรม ซึ่งสามารถระบุตัวตนได้ไม่ว่าทางตรงหรือทางอ้อม เพื่อใช้ในการกระทำความผิดทางเทคโนโลยีหรืออาชญากรรมอื่น ๆ จะมีโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ และหากมีลักษณะของการซื้อขาย แลกเปลี่ยน หรือแสวงหาผลประโยชน์จากข้อมูลโดยมิชอบ โทษจะเพิ่มขึ้นเป็นจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ หลักกฎหมายดังกล่าวมีจุดมุ่งหมายเพื่อการคุ้มครองข้อมูลของผู้ถึงแก่กรรมที่มักถูกมิจฉาชีพนำไปแอบอ้าง เนื่องจากผู้เสียชีวิตไม่สามารถปกป้องสิทธิของตนเองได้ การกำหนดบทลงโทษที่ชัดเจนจึงเป็นมาตรการสำคัญในการป้องกันอาชญากรรมตั้งแต่ต้นทางพร้อมทั้งควบคุมทั้งผู้ที่ใช้ข้อมูลโดยตรงและผู้ที่มีส่วนเกี่ยวข้อ ง ในการเปิดเผยหรือเผยแพร่ข้อมูลด้วยเจตนาร่วมในการกระทำความผิด

ดังนั้น พระราชกำหนดฉบับนี้จึงเป็นการปรับปรุงกฎหมายให้สอดรับกับเทคโนโลยีและภัยคุกคามในยุคดิจิทัล โดยเน้นควบคุมการใช้บริการโทรคมนาคม ป้องกันการเปิดบัญชีและทำธุรกรรมผิดกฎหมาย จัดตั้งหน่วยงานเฉพาะกิจที่มีหน้าที่และอำนาจในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีอย่างเป็นระบบ เพิ่มความรับผิดของผู้ประกอบธุรกิจ และกำหนดกลไกคืนเงินให้ผู้เสียหาย มาตรการเหล่านี้ช่วยเสริมประสิทธิภาพในการปราบปรามอาชญากรรมทางเทคโนโลยีและคุ้มครองสิทธิประชาชนได้อย่างเป็นรูปธรรม

ส่วนที่ 3
ข้อมูลประกอบการพิจารณา

1. เทคโนโลยีการยืนยันตัวตน[1]

เทคโนโลยีการยืนยันตัวตน (Identity Verification) ได้รับการพัฒนาอย่างมากในปัจจุบัน โดยมีการใช้งานทั้งแบบออฟไลน์และออนไลน์ ซึ่งการยืนยันตัวตนแบบอิเล็กทรอนิกส์ เช่น Electronic Know Your Customer (e-KYC) และ National Digital ID (NDID) ได้กลายเป็นกระบวนการสำคัญที่ช่วยสร้างความมั่นใจในการทำธุรกรรมออนไลน์และการใช้บริการดิจิทัล โดยเฉพาะในภาคธุรกิจและการเงิน การยืนยันตัวตนไม่เพียงแต่ช่วยป้องกันการฉ้อโกงเท่านั้น แต่ยังเป็นกลไกสำคัญในการสร้างความน่าเชื่อถือและความปลอดภัยในโลกดิจิทัลอีกด้วย

ข้อดีของการยืนยันตัวตน

การทำธุรกรรมออนไลน์ การยืนยันตัวตนเป็นกลไกสำคัญในการสร้างความปลอดภัยและความน่าเชื่อถือให้กับทั้งผู้ให้บริการและผู้ใช้บริการ ระบบยืนยันตัวตนที่มีประสิทธิภาพไม่เพียงแต่ช่วยป้องกันการฉ้อโกงและควบคุมกิจกรรมหรือธุรกรรมที่ผิดกฎหมายเท่านั้น แต่ยังเพิ่มประสิทธิภาพการดำเนินธุรกิจและสร้างความเชื่อมั่นให้กับลูกค้า

1) เพิ่มความปลอดภัยในการทำธุรกรรมออนไลน์

องค์กรสามารถตรวจสอบตัวตนของผู้ทำธุรกรรมก่อนอนุมัติการดำเนินการ เพื่อให้ธุรกรรมดังกล่าวเป็นไปอย่างถูกต้อง นอกจากนี้ การยืนยันตัวตนแบบอิเล็กทรอนิกส์ เช่น e-KYC ถือเป็นเกราะป้องกันที่ช่วยลดความเสี่ยงจากการเข้าถึงบัญชีธุรกรรมหรือข้อมูลที่มีความอ่อนไหวโดยไม่ได้รับอนุญาต อีกทั้งยังมีการบันทึกประวัติการทำธุรกรรมเพื่อการตรวจสอบย้อนหลัง และเพิ่มความปลอดภัยโดยรวมในการโอนเงินระหว่างบัญชี

2) ลดความเสี่ยงจากการฉ้อโกงและการขโมยข้อมูล

เทคโนโลยีการยืนยันตัวตนที่มีประสิทธิภาพสามารถช่วยป้องกันการฉ้อโกงในหลายรูปแบบ ตั้งแต่การตรวจจับและป้องกันการปลอมแปลงเอกสาร ไปจนถึงการป้องกันการสร้างบัญชีปลอมเพื่อทำธุรกรรมผิดกฎหมาย อีกทั้งยังช่วยลดความเสี่ยงจากการขโมยข้อมูลส่วนบุคคล และป้องกันการฟอกเงินผ่านช่องทางออนไลน์ที่สำคัญ คือ องค์กรสามารถตรวจจับและดำเนินการเมื่อพบพฤติกรรมที่น่าสงสัย ช่วยให้สามารถจัดการกับภัยคุกคามได้อย่างทันท่วงที

3) สร้างความน่าเชื่อถือในการใช้บริการดิจิทัล

การที่ธุรกิจมีระบบยืนยันตัวตนที่ได้มาตรฐานอย่างการยืนยันตัวตน NDID, e-KYC หรือ Biometrics สามารถสร้างความน่าเชื่อถือให้แก่ธุรกิจได้ เพราะแสดงให้เห็นถึงการให้ความสำคัญกับความปลอดภัยและความเป็นส่วนตัวของลูกค้า ผู้ใช้บริการจึงมั่นใจในการทำธุรกรรมมากขึ้น ในอีกมุมหนึ่งการยืนยันตัวตนยังช่วยสร้างความโปร่งใสในการดำเนินธุรกิจ ส่งผลให้ธุรกิจสามารถเสริมสร้างความสัมพันธ์ สร้าง Brand Loyalty หรือความภักดีต่อแบรนด์ในระยะยาวได้อีกด้วย

---

[1] SCB TechX Admin. (29 ตุลาคม 2567). **การยืนยันตัวตน สำคัญต่อธุรกิจอย่างไร มีกี่วิธีที่องค์กรประยุกต์ใช้ได้**. สืบค้น 19 พฤษภาคม 2568 จาก https://scbtechx.io/th/blogs/identity-verification-ekyc-ndid-for-business/

4) เพิ่มประสิทธิภาพในการให้บริการของธุรกิจ

ระบบยืนยันตัวตนดิจิทัลสามารถช่วยปรับปรุงประสิทธิภาพการดำเนินงานขององค์กรอย่างมีนัยสำคัญ ยกตัวอย่างเช่น กระบวนการตรวจสอบเอกสาร ที่แต่เดิมเคยใช้เวลานาน ปัจจุบันสามารถทำได้ในเวลาไม่กี่นาที ผ่านระบบยืนยันตัวตน ซึ่งช่วยประหยัดต้นทุนการดำเนินงานในระยะยาว นอกจากนี้ยังช่วยเพิ่มความเร็วในการอนุมัติบริการ ลดความผิดพลาดของมนุษย์ (Human Error) ในการป้อนข้อมูลด้วยมือ และช่วยให้องค์กรสามารถจัดการข้อมูลลูกค้าได้อย่างมีประสิทธิภาพมากขึ้น

วิธีการยืนยันตัวตน

การยืนยันตัวตนในปัจจุบันมีหลากหลายวิธี ซึ่งแต่ละวิธีมีจุดเด่นและข้อดีที่แตกต่างกันไป ซึ่งการเลือกใช้วิธีการยืนยันตัวตนที่เหมาะสมขึ้นอยู่กับประเภทของธุรกิจ ระดับความปลอดภัยที่ต้องการ และความสะดวกในการใช้งานของผู้ใช้บริการ

1) การยืนยันตัวตนแบบ Knowledge-Based

การยืนยันตัวตนแบบ Knowledge-Based เป็นวิธีการพื้นฐานที่อาศัยข้อมูลที่ผู้ใช้งานเท่านั้นที่ควรทราบ โดยเป็นการให้ผู้ใช้งานตั้งรหัสผ่านที่มีเฉพาะตนเองที่รู้ หรืออาจเป็นการตั้งคำถามเฉพาะบุคคล เช่น “ชื่อโรงเรียนประถมของคุณคืออะไร?” บางระบบใช้การตั้งคำถามเพื่อความปลอดภัยหลายข้อ ร่วมกับการใช้ข้อมูลประวัติส่วนตัวที่เฉพาะเจาะจง วิธีการยืนยันตัวตนแบบ Knowledge-Based มีข้อดี คือ ง่ายต่อการใช้งานและไม่ต้องใช้อุปกรณ์เพิ่มเติม แต่ก็มีข้อเสียคือ เสี่ยงต่อการถูกคาดเดา ซึ่งอาจนำไปสู่การถูกขโมยข้อมูลได้

2) การยืนยันตัวตนแบบ Two-Factor Authentication (2FA)

Two-Factor Authentication เป็นการเพิ่มชั้นความปลอดภัยด้วยการยืนยันสองขั้นตอน โดยทั่วไปจะใช้การส่งรหัส OTP ผ่าน SMS หรืออีเมล ร่วมกับการใช้แอปพลิเคชันยืนยันตัวตนเฉพาะ เช่น Google Authenticator บางระบบอาจใช้อุปกรณ์ Security Key หรือการยืนยันผ่านการแจ้งเตือนบนมือถือ ซึ่งวิธีนี้ให้ความปลอดภัยสูงขึ้น แต่ผู้ใช้จำเป็นต้องมีอุปกรณ์เสริมหรือโทรศัพท์มือถือในการยืนยันตัวตน

3) การยืนยันตัวตนด้วย Biometrics

Biometric หมายถึง ข้อมูลชีวภาพ โดยเป็นการใช้ลักษณะทางกายภาพที่เป็นเอกลักษณ์ของแต่ละบุคคล เพื่อยืนยันตัวตน เช่น การสแกนลายนิ้วมือ การสแกนใบหน้าด้วยเทคโนโลยี 3D Mapping หรือการสแกนม่านตาด้วยระบบอินฟราเรด ซึ่งทั้งหมดล้วนมีความแม่นยำสูง ป้องกันการปลอมแปลงได้ดี นอกจากนี้ยังมีการใช้เทคโนโลยีการจดจำเสียงด้วย AI แม้วิธีนี้จะมีความปลอดภัยสูง แต่ก็มีข้อจำกัดด้านต้นทุนและความจำเป็นในการติดตั้งอุปกรณ์พิเศษเพิ่มเติม

4) การยืนยันตัวตนแบบ e-KYC

Electronic Know Your Customer (e-KYC) เป็นระบบการพิสูจน์และยืนยันตัวตนทางอิเล็กทรอนิกส์ที่ครบวงจร โดยเริ่มจากการเก็บและตรวจสอบหลักฐานเอกสารประกอบการยืนยันตัวตน เช่น บัตรประชาชน หนังสือเดินทาง ผ่านการถ่ายภาพ พร้อมตรวจสอบความถูกต้อง โดยระบบจะทำการเปรียบเทียบภาพถ่ายกับฐานข้อมูลทางการและตรวจสอบข้อมูลกับหน่วยงานราชการเพื่อยืนยันตัวตน พร้อมทั้งมีระบบป้องกันการปลอมแปลงเอกสาร วิธีนี้มีความน่าเชื่อถือสูงและเป็นที่ยอมรับตามกฎหมาย

5) การยืนยันตัวตนผ่านระบบ NDID

National Digital ID (NDID) หรือระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลแห่งชาติ ที่เป็นแพลตฟอร์มกลางของประเทศไทย หรือ บริษัท เนชั่นแนลดิจิทัลไอดี จำกัด (National Digital ID Co., Ltd.) โดยเป็นโครงสร้างพื้นฐานสำคัญที่เชื่อมโยงข้อมูลระหว่างสถาบันการเงินและหน่วยงานรัฐ ระบบนี้ใช้มาตรฐานความปลอดภัยระดับสูงและรองรับการทำธุรกรรมระหว่างหน่วยงาน ช่วยลดความซ้ำซ้อนในการยืนยันตัวตน และมีระบบการรักษาความปลอดภัยข้อมูลแบบรวมศูนย์

ตัวอย่างองค์กรที่ใช้การยืนยันตัวตนบนโลกดิจิทัล

ในปัจจุบัน องค์กรจากหลากหลายอุตสาหกรรมได้นำระบบการยืนยันตัวตนดิจิทัลมาใช้เพื่อเพิ่มความปลอดภัยและประสิทธิภาพในการให้บริการ โดยแต่ละองค์กรมีรูปแบบการประยุกต์ใช้ที่แตกต่างกันตามความต้องการ

1) ธุรกิจอีคอมเมิร์ซ แพลตฟอร์มอีคอมเมิร์ซอย่าง Shopee และ Lazada ใช้ระบบยืนยันตัวตนเพื่อสร้างความปลอดภัยในการซื้อขายออนไลน์ โดยมีการนำไปใช้ในหลายขั้นตอน เช่น การลงทะเบียนผู้ขาย - ร้านค้าต้องผ่านการยืนยันตัวตนด้วย e-KYC เพื่อยืนยันตัวตนและป้องกันการฉ้อโกง โดยต้องกรอกข้อมูลส่งเอกสารยืนยันตัวตน และหลักฐานทางธุรกิจ การชำระเงิน - ระบบจะมีการยืนยันตัวตนผู้ซื้อก่อนทำการชำระเงิน โดยเฉพาะเมื่อมีการใช้บัตรเครดิตหรือการโอนเงินจำนวนมาก การคุ้มครองผู้บริโภค - การยืนยันตัวตนช่วยในการติดตามและแก้ไขปัญหากรณีเกิดข้อพิพาทระหว่างผู้ซื้อและผู้ขาย

2) สถาบันทางการแพทย์และโรงพยาบาล

โรงพยาบาลและคลินิกต่าง ๆ ได้นำระบบยืนยันตัวตนมาใช้เพื่อปกป้องข้อมูลทางการแพทย์ที่มีความอ่อนไหว ตั้งแต่การเข้าถึงประวัติการรักษา โดยผู้ป่วยสามารถยืนยันตัวตนผ่านระบบ Biometric หรือ 2FA ก่อนเข้าถึงประวัติการรักษาออนไลน์ การนัดหมายแพทย์ ไปจนถึงการรักษาทางไกล (Telemedicine) เพื่อรับรองว่าการรักษาและการจ่ายยาเป็นไปอย่างถูกต้องและปลอดภัย

3) สถาบันการเงินและธนาคาร

ธนาคารและสถาบันการเงินได้มีการนำเทคโนโลยีการยืนยันตัวตนที่ทันสมัยมาใช้เพื่อยกระดับความปลอดภัยในการทำธุรกรรม เช่น การเปิดบัญชีออนไลน์ โดยธนาคารใช้ระบบ e-KYC ที่รวมการถ่ายภาพบัตรประชาชน การถ่ายภาพใบหน้า และการตรวจสอบ Liveness Detection เพื่อเปิดบัญชีโดยไม่ต้องไปสาขา การใช้การยืนยันตัวตนหลายขั้นตอน เช่น รหัส OTP ร่วมกับการสแกนลายนิ้วมือหรือใบหน้าสำหรับธุรกรรมที่มีมูลค่าสูงไปจนถึงการขอสินเชื่อออนไลน์ เพื่อประเมินความน่าเชื่อถือของผู้ขอสินเชื่อและป้องกันการฉ้อโกง

จะเห็นได้ว่าการยืนยันตัวตนในโลกดิจิทัลมีบทบาทสำคัญในการสร้างความปลอดภัยและความน่าเชื่อถือให้กับธุรกิจและบริการต่าง ๆ และด้วยเทคโนโลยีที่ก้าวหน้าในปัจจุบัน ทำให้การยืนยันตัวตนมีความแม่นยำและสะดวกมากขึ้น องค์กรที่นำระบบการยืนยันตัวตนที่มีประสิทธิภาพมาใช้จะได้เปรียบในการแข่งขันและสร้างความเชื่อมั่นให้กับลูกค้า โดยเฉพาะอย่างยิ่งในยุคที่การทำธุรกรรมดิจิทัลมีการเติบโตอย่างรวดเร็วและต่อเนื่อง

2. การปราบปรามอาชญากรรมทางเทคโนโลยีของภาครัฐ

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอี)[2] เป็นประธานการประชุมคณะกรรมการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ครั้งที่ 2/2568 โดยระบุว่า รัฐบาลให้ความสำคัญกับการแก้ปัญหาอาชญากรรมออนไลน์อย่างจริงจัง เนื่องจากส่งผลกระทบต่อประชาชนในวงกว้าง

ในการประชุมครั้งนี้ ได้พิจารณาผลการดำเนินงานและมาตรการเร่งด่วนในการแก้ปัญหาอาชญากรรมออนไลน์ 6 ประเด็นสำคัญ ซึ่งมีความคืบหน้าจนถึงวันที่ 17 มีนาคม 2568 สรุปได้ดังนี้

2.1 การปราบปรามจับกุมคดีอาชญากรรมออนไลน์ (เดือนกุมภาพันธ์ 2568)

ประเภทคดี	จำนวนจับกุม (ก.พ. 68)	ค่าเฉลี่ยต่อเดือน (ม.ค.-มี.ค. 67)	เพิ่มขึ้น (ร้อยละ)
คดีอาชญากรรมทางเทคโนโลยี (รวมทุกประเภท)	4,505 ราย	2,495 ราย	+ ร้อยละ 80.56
คดีพนันออนไลน์	2,069 ราย	1,064 ราย	+ ร้อยละ 94.45
คดีบัญชีม้า / ซิมม้า / ความผิดตาม พ.ร.ก.	325 ราย	240 ราย	+ร้อยละ 35.42

2.2 การปิดโซเชียลมีเดีย เว็บผิดกฎหมาย และเว็บพนันออนไลน์ (ผลการดำเนินงานที่สำคัญถึง 28 กุมภาพันธ์ 2568)

การระงับบัญชีที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี

ประเภทการปิดกั้น	จำนวน URLs
เว็บไซต์พนันออนไลน์	33,094
เว็บไซต์หลอกลวงออนไลน์	1,130

การประสานแพลตฟอร์มเพื่อขอปิดกั้นเว็บไซต์หลอกลวงออนไลน์

ประเภทคำสั่ง	จำนวน URLs
มีคำสั่งศาล	7,338
ไม่มีคำสั่งศาล	21,335

[2] ดีอี เปิด สถิติอาชญากรรมออนไลน์ ยอดจับกุมเดือนละ 2,495 คน. (20 มีนาคม 2568). **ประชาชาติธุรกิจออนไลน์**. สืบค้น 19 พฤษภาคม 2568 จาก https://www.prachachat.net/ict/news-1777028

2.3 การแก้ปัญหาบัญชีม้า เร่งอายัด ตัดตอนการโอนเงิน (ผลการดำเนินงานที่สำคัญถึง 28 กุมภาพันธ์ 2568)

หน่วยงานที่ดำเนินการ	จำนวนบัญชีที่ระงับ
AOC ระงับบัญชีชั่วคราว	337,690
ธนาคารระงับบัญชี	997,600
รวมทั้งหมด	**1,335,290**

มาตรการปลดบัญชีม้าและการป้องกันอาชญากรรมทางการเงิน ที่ประชุมคณะกรรมการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้เห็นชอบแนวทางจัดการบัญชีม้า โดยแบ่งออกเป็น 2 ประเภทหลัก ได้แก่ บัญชี “ม้าดำ” มอบอำนาจให้สำนักงานป้องกันและปราบปรามการฟอกเงิน (สำนักงาน ปปง.) ซึ่งเป็นหน่วยงานเดียวที่สามารถปลดล็อกบัญชีได้เป็นผู้รับผิดชอบดำเนินการ บัญชี “ม้าเทา” มอบอำนาจให้กองบัญชาการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) เป็นผู้รับผิดชอบดำเนินการ

ผู้ที่ถูกกล่าวหาว่ามีความเกี่ยวข้องกับบัญชีม้า และมีบัญชีมากกว่า 1 บัญชี สามารถยื่นเรื่องต่อกองบัญชาการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) เพื่อขอปลดล็อกบัญชีบางส่วนหรือขอเปิดบัญชีใหม่ได้ 1 บัญชี เรียกว่า “บัญชีเพื่อการยังชีพ” ซึ่งจะใช้ได้เฉพาะการทำธุรกรรมผ่านธนาคารเท่านั้น ไม่สามารถใช้ทำธุรกรรมออนไลน์ได้

มาตรการป้องกันอาชญากรรมทางการเงินในธุรกิจสินทรัพย์ดิจิทัล สำนักงานป้องกันและปราบปรามการฟอกเงิน (สำนักงาน ปปง.), สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) และสมาคมผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลไทย ได้ร่วมกันหารือเพื่อเชื่อมโยงข้อมูลเกี่ยวกับบัญชีม้า โดยมีการประกาศรายชื่อ HR-03 และกำหนดแนวทางตรวจสอบธุรกรรมสินทรัพย์ดิจิทัลที่มีความเสี่ยง เพื่อป้องกันไม่ให้มิจฉาชีพใช้ช่องทางสินทรัพย์ดิจิทัลในการฟอกเงินหรือกระทำความผิด

2.4 การแก้ไขปัญหาซิมม้า ซิมบุคคลต่างด้าว (ผลการดำเนินงานที่สำคัญถึง 28 กุมภาพันธ์ 2568)

สรุปข้อมูลการแก้ไขปัญหาซิมม้าและซิมบุคคลต่างด้าวได้เป็น 3 หัวข้อหลัก ดังนี้

1) การตรวจสอบซิมแบบเติมเงินที่โทรออกเกิน 100 ครั้ง/วัน

รายการ	จำนวนเลขหมาย (สะสม)
ซิมที่ถูกระงับบริการ	233,338
ผู้มาแสดงตนแล้ว	441
ยังไม่มาแสดงตน	232,897

2) กลุ่มผู้ถือครองซิม 101 เลขหมายขึ้นไป

รายการ	จำนวนเลขหมาย
รวมเลขหมายที่เข้าข่ายตรวจสอบ	5,078,283
ยืนยันตัวตนแล้ว	4,273,918
คงเหลือที่ยังต้องยืนยัน	804,365

3) กลุ่มผู้ถือครองซิม 6-100 เลขหมาย

รายการ	จำนวนเลขหมาย
รวมเลขหมายที่เข้าข่ายตรวจสอบ	3,981,251
ยืนยันตัวตนแล้ว	2,424,402
คงเหลือที่ยังต้องยืนยัน	1,556,849

มาตรการควบคุมการลงทะเบียนซิมการ์ดและการส่งข้อความ SMS ที่แนบลิงก์ ที่ประชุมคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ได้ออกมาตรการใหม่เพื่อป้องกันการใช้ซิมการ์ดในทางที่ผิด โดยเฉพาะจากกลุ่มผู้ไม่มีสัญชาติไทย ดังนี้

สำหรับผู้ไม่มีสัญชาติไทยที่ต้องการลงทะเบียนใช้งานซิมการ์ด จะต้องใช้หนังสือเดินทาง (Passport) เป็นเอกสารแสดงตน และสามารถลงทะเบียนได้ไม่เกิน 3 เลขหมายต่อผู้ให้บริการโทรศัพท์มือถือ 1 ราย ในส่วนของระบบการตรวจสอบอัตลักษณ์ (Biometrics) ได้กำหนดให้ผู้ให้บริการโทรศัพท์มือถือปรับปรุงระบบให้สามารถตรวจจับการปลอมแปลงตัวตนได้ ด้วยเทคโนโลยี “Liveness Detection” โดยต้องดำเนินการให้แล้วเสร็จภายใน 180 วัน นับตั้งแต่วันที่ 19 กุมภาพันธ์ 2568 นอกจากนี้ ยังมีมาตรการควบคุมการส่ง SMS ที่มีลิงก์แนบโดยสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และผู้ให้บริการโทรคมนาคม ได้ร่วมกันกำกับดูแลให้มีการลงทะเบียนชื่อผู้ส่ง (Sender Name) อย่างเป็นระบบ ปัจจุบันมีการลงทะเบียนแล้วกว่า 100,000 รายการ จากผู้ให้บริการทั้งหมด 42 ราย แบ่งเป็นผู้ที่ลงทะเบียนแล้ว 25 ราย อยู่ระหว่างดำเนินการ 4 ราย และไม่มีบริการส่งข้อความแนบลิงก์ 13 ราย

มาตรการทั้งหมดนี้มีเป้าหมายเพื่อเสริมสร้างความปลอดภัยในการใช้บริการโทรศัพท์มือถือและลดความเสี่ยงจากอาชญากรรมทางเทคโนโลยีที่อาศัยช่องทางโทรคมนาคม

2.5 การจัดระเบียบเสาโทรคมนาคมและสายสัญญาณบริเวณชายแดน

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ได้ลงพื้นที่ตรวจสอบการติดตั้งเสาโทรคมนาคม สายอินเทอร์เน็ต และสายโทรศัพท์ที่อาจผิดกฎหมายตามแนวชายแดนประเทศเพื่อนบ้าน โดยดำเนินการกำหนดมาตรฐานทั้งในด้านความสูงของเสา และค่าความแรงของสัญญาณ เพื่อป้องกันการใช้งานผิดวัตถุประสงค์หรือข้ามพรมแดน

2.6 การศึกษามาตรการควบคุมดูแลแพลตฟอร์ม OTT

ที่ประชุมคณะกรรมการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้มอบหมายให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ร่วมกับสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) จัดตั้งคณะทำงานเพื่อศึกษาการออกมาตรการควบคุมดูแลแพลตฟอร์ม OTT (Over-The-Top) ซึ่งเป็นบริการสตรีมมิ่งออนไลน์ที่ผู้ใช้งานสามารถเข้าถึงเนื้อหา เช่น ภาพยนตร์ รายการทีวี เพลง หรือพอดแคสต์ ได้โดยตรงผ่านอินเทอร์เน็ต โดยไม่ผ่านผู้ให้บริการเครือข่ายแบบดั้งเดิม ตัวอย่างแพลตฟอร์ม ได้แก่ Netflix, YouTube, Disney+, TikTok และ Spotify แม้บริการเหล่านี้

จะอำนวยความสะดวกและสร้างประโยชน์ด้านความบันเทิงและข้อมูล แต่ก็อาจถูกนำไปใช้ในทางที่ผิด เช่น การหลอกลวงออนไลน์ การเผยแพร่เนื้อหาที่ไม่เหมาะสม หรือการละเมิดลิขสิทธิ์ ซึ่งสร้างความเสียหายต่อประชาชนเพื่อจัดระเบียบและกำกับดูแลแพลตฟอร์ม OTT อย่างเหมาะสม จึงมีการเสนอแนวทางมาตรการหลัก 5 ด้าน ได้แก่

1. มาตรการด้านความปลอดภัย

ป้องกันการละเมิดลิขสิทธิ์ และการเข้าถึงเนื้อหาที่ผิดกฎหมาย รวมถึงกำหนดให้มีการยืนยันตัวบุคคล เพื่อป้องกันการนำแพลตฟอร์มไปใช้ในทางที่ไม่เหมาะสม

2. การออกระเบียบกำกับด้านเนื้อหา

ปรับปรุงกฎหมายเพื่อให้สามารถควบคุมเนื้อหาบนแพลตฟอร์ม OTT ได้อย่างมีประสิทธิภาพ กำหนดให้แพลตฟอร์มต่างประเทศที่ให้บริการในประเทศไทยต้องขอใบอนุญาตและอยู่ภายใต้กฎหมายไทย รวมถึงผลักดันแนวทางการกำกับดูแลในระดับสากล

3. การส่งเสริมอุตสาหกรรมดิจิทัลและการจัดเก็บภาษี

สนับสนุนผู้ประกอบการไทยในการพัฒนาแพลตฟอร์มของตนเอง กำหนดให้แพลตฟอร์ม OTT ที่มีรายได้จากผู้ใช้งานในไทยต้องเสียภาษีในประเทศ และส่งเสริมการสร้างมูลค่าเพิ่มในเศรษฐกิจดิจิทัลภายในประเทศ

4. การคุ้มครองข้อมูลส่วนบุคคล

แพลตฟอร์ม OTT ต้องปฏิบัติตามมาตรฐานการคุ้มครองข้อมูล เช่น GDPR ของยุโรป และต้องมีระบบควบคุมการเก็บ ใช้ และจัดการข้อมูลผู้ใช้อย่างเหมาะสม เพื่อคุ้มครองสิทธิความเป็นส่วนตัวของประชาชน

5. การกำกับดูแลด้านการแข่งขัน

ป้องกันการผูกขาดของแพลตฟอร์มขนาดใหญ่ที่อาจส่งผลต่อการแข่งขันอย่างไม่เป็นธรรม พร้อมสนับสนุนการพัฒนาแพลตฟอร์มท้องถิ่น และส่งเสริมความหลากหลายในการแข่งขันในตลาดดิจิทัล

3. มาตรการทางกฎหมายแก้ไขปัญหามิจฉาชีพออนไลน์ของประเทศต่าง ๆ[3]

ข้อมูลจาก The Global State of Scam Report รายงานสถิติในปี 2564 ว่ามีผู้คนทั่วโลกที่ถูกมิจฉาชีพหลอกลวงเป็นมูลค่าความเสียหายถึง 55.3 พันล้านดอลลาร์สหรัฐ ซึ่งในจำนวนนั้นเป็นการหลอกลวงเงินผ่านออนไลน์ 293 ล้านครั้ง สูงกว่าปีที่ผ่านมาร้อยละ 10.2 ขณะที่ข้อมูลจาก ACI Worldwide รายงานว่าในปี 2565 ไทยอยู่ในอันดับที่ 6 ที่ถูกหลอกลวงทางการเงิน โดยมีจำนวนมากถึง 16.5 พันล้านรายการ เมื่อสำรวจการเกิดปัญหาภัยทุจริตทางการเงินพบว่าหลายประเทศตกเป็นเหยื่อมิจฉาชีพเช่นเดียวกัน บางประเทศมีกลไกในการป้องกันและแก้ไขปัญหา อย่างไรก็ตามมีเพียงบางประเทศเท่านั้นที่มีมาตรการ กฎหมายในการเยียวยาความเสียหาย

[3] **แก้เกมมิจฉาชีพคุกคาม บทเรียนจาก ตปท. อุดช่องโหว่ทาง กม**. (9 มกราคม 2567). สืบค้น 19 พฤษภาคม 2568 จาก https://www.tcc.or.th/09012567_online-fruad_article-midi/

มาเลเซีย มาเลเซียประเทศเพื่อนบ้านในอาเซียนของไทย พบความเสียหายจากภัยทางการเงินออนไลน์ในช่วงระหว่างปี 2553-2564 กว่า 3.3 พันล้านริงกิตมาเลเซีย (ประมาณ 7.5 หมื่นล้านบาท) เมื่อมีการจับตัวผู้กระทำความผิดพบว่าส่วนมากเกิดจากการเปิดบัญชีม้า โดยในปี 2564 พบบัญชีม้าถึง 29,769 บัญชี เพื่อป้องกันปัญหาดังกล่าว รัฐบาลมาเลเซียได้กำหนดมาตรการ ดังนี้

มาตรการด้านกฎหมาย รัฐบาลมาเลเซียได้ออกกฎหมายกำหนดให้การเปิดบัญชีม้าเป็นความผิดตามประมวลกฎหมายอาญามีโทษทั้งจำทั้งปรับ นอกจากนี้มาเลเซียยังมีวิธีการเตือนภัยที่น่าสนใจ คือ ธนาคารกลาง (Bank Negara Malaysia) ได้จัดทำระบบฐานข้อมูล “การแจ้งเตือนภัยทางการเงิน (Financial Consumer Alert List)” ผ่านเว็บไซต์ของธนาคารกลางเปิดเผยรายชื่อเว็บไซต์หรือรายชื่อผู้ประกอบธุรกิจที่ต้องระมัดระวัง โดยรายชื่อมาจากธนาคารต่าง ๆ ส่งข้อมูลบัญชีม้าเข้าสู่แพลตฟอร์ม “Semak mule” ซึ่งเป็นแฟลตฟอร์มที่แจ้งข้อมูลเรื่องนี้โดยเฉพาะ และธนาคารกลางยังทำโครงการให้ความรู้เรื่องทางการเงินแก่ผู้บริโภคให้เท่าทันกับภัยทางการเงินเป็นยุทธศาสตร์ควบคู่กันไปด้วย

มาตรการแก้ไขปัญหา มาเลเซียมีการตั้งศูนย์ตอบโต้การหลอกลวงแห่งชาติ (The National Scam Response Center: NSRC) โดยรวบรวมบุคลากรหลายหน่วยงานที่มีความรู้ความสามารถ เพื่อประสานงานช่วยเหลือแก้ไขปัญหาภัยทางการเงินออนไลน์ ผ่านเบอร์โทรศัพท์เพียงหมายเลขเดียว อย่างไรก็ตาม การเยียวยาความเสียหายจากภัยทางการเงินออนไลน์มาเลเซียก็ยังไม่มีกฎหมายกำหนดไว้ ผู้บริโภคต้องฟ้องดำเนินคดีกับธนาคารเพื่อเรียกเงินคืนเอง

เกาหลีใต้ เกาหลีใต้อีกหนึ่งประเทศในเอเชียตะวันออกที่พบปัญหาภัยทางการเงินเช่นเดียวกัน

มาตรการด้านกฎหมาย ให้ธนาคารสามารถระงับการโอนเงินและการถอนเงินออกจากบัญชีมิจฉาชีพได้ ส่วนมากปัญหาภัยทางการเงินที่พบในเกาหลีใต้เกิดจากฟิชชิ่ง (Fishing scams คือ การสร้างสถานการณ์โดยการส่งข้อความ อีเมล หรือเว็บไซต์ปลอม เพื่อเป็นเหยื่อล่อให้ผู้ใช้งานเข้ามาติดเบ็ด และหลอกล่อผู้ใช้ให้กรอกข้อมูลส่วนตัวต่าง ๆ หรือส่งโปรแกรมให้ติดตั้งลงเครื่องคอมพิวเตอร์ตามที่แฮกเกอร์ต้องการ) โดยข้อมูลขององค์กรกำกับดูแลทางบริการด้านการเงิน ชื่อว่า Financial Supervisory Service (FSS) พบว่า ปี 2565 มีจำนวนผู้เสียหาย 1,879 ราย ความเสียหายกว่า 145 พันล้านวอน (ประมาณ 37 ล้านบาท) แต่มีผู้เสียหายได้เงินคืนเพียงร้อยละ 26.1 เท่านั้น หน่วยงานรัฐจึงมีแนวคิดให้ธนาคารต้องร่วมรับผิดชอบชดใช้เงินคืนบางส่วนให้แก่ผู้บริโภคที่ได้รับความเสียหายจากการถูกหลอกลวงออนไลน์ในรูปแบบของการฟิชชิ่ง แต่หากเกิดความเสียหายจากการหลอกลวงกรณีอื่น ๆ ยังไม่มีแนวทางเยียวยาความเสียหายที่ชัดเจน

สหราชอาณาจักร

ปี 2564 สหราชอาณาจักรพบความเสียหายจากการหลอกลวงออนไลน์คิดเป็นมูลค่ากว่า 583.2 ล้านปอนด์ (ประมาณ 2.5 หมื่นล้านบาท) จึงตั้งหน่วยสืบหาข้อมูลด้านการหลอกลวงแห่งชาติ (The National Fraud Intelligence Bureau) เป็นศูนย์กลางในการแก้ไขปัญหาภัยทางการเงินแบบรวมศูนย์ โดยประสานงานกับตำรวจและหน่วยงานที่เกี่ยวข้อง สหราชอาณาจักรมีกลไกเยียวยาความเสียหายที่น่าสนใจ คือ จรรยาบรรณภาคสมัครใจเรียกว่า Authorised push payment Scam Code (APP Code) ที่กำหนดให้ธนาคารเยียวยาความเสียหายโดยรับผิดชอบร่วมกันคนละครึ่งระหว่างธนาคารที่โอนเงินและธนาคารที่รับโอนเงิน เพื่อให้ผู้บริโภคที่ได้รับความเสียหายได้รับเงินคืนเต็มจำนวนภายใน 5 วันหลังแจ้งเหตุถูกหลอกลวง ซึ่งเป็นความสมัครใจของธนาคารที่เข้าร่วมจรรยาบรรณดังกล่าว นอกจากนี้ สหราชอาณาจักรพัฒนา APP Code เป็นกฎหมาย

มีผลบังคับใช้ภายในปี 2567 ส่วนในอังกฤษมีการนำเทคโนโลยีปัญญาประดิษฐ์หรือ เอไอ (AI) มาวิเคราะห์พฤติกรรมการเงินของลูกค้าและข้อมูลสำคัญต่าง ๆ ทำให้ธนาคารสามารถระงับธุรกรรมต้องสงสัยได้อย่างทันท่วงที

ออสเตรเลีย

ปี 2565 ออสเตรเลียพบความเสียหายจากภัยทางการเงินมูลค่า 3 พันล้านดอลลาร์ออสเตรเลีย (ประมาณ 6.9 หมื่นล้านบาท)

มาตรการแก้ไขปัญหา มีการตั้งศูนย์ต่อต้านการฉ้อโกงทางออนไลน์แห่งชาติ (National Anti-Scam Center) เพื่อแก้ไขปัญหาเรื่องร้องเรียน ประสานงานหน่วยงานที่เกี่ยวข้อง ส่งต่อข้อมูลฉ้อโกงให้หน่วยงาน ประชาชน ผู้ประกอบการรายอื่นรับทราบ เพื่อหยุดการทำธุรกรรม ตลอดจนทำระบบแจ้งเบาะแส แจ้งเตือนภัย ประชาสัมพันธ์และให้ความรู้ผู้บริโภค นอกจากนี้ยังให้หน่วยงานที่เกี่ยวกับการสื่อสารและเทคโนโลยีติดตามตรวจสอบสกัดกั้น Call Center และข้อความ (SMS) หลอกลวงด้วย แต่ออสเตรเลียยังไม่มีแนวทางเยียวยาให้ธนาคารรับผิดชอบความเสียหายแก่ผู้บริโภคที่เป็นเหยื่อของมิจฉาชีพแต่อย่างใด

ไทย ตั้งแต่ปี 2565 ถึง 2566 พบความเสียหายจากภัยทางการเงินกว่า 4.3 หมื่นล้านบาท

มาตรการด้านกฎหมาย ในช่วงต้นปี 2566 ภาครัฐตราพระราชกำหนดปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ให้อำนาจธนาคารระงับการโอนเงินอายัดบัญชีได้ทันทีเมื่อต้องสงสัยเป็นคนร้ายหรือบัญชีม้า รวมถึงกำหนดโทษทั้งจำทั้งปรับเอาผิดเจ้าของบัญชีม้า ผู้ซื้อขายซิมม้า และให้ธนาคารแลกเปลี่ยนข้อมูลกับหน่วยงานที่เกี่ยวข้อง เช่น สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน สมาคมธนาคารไทย เพื่อช่วยเหลือเหยื่อและตามจับกุมคนร้ายให้รวดเร็วขึ้น

มาตรการแก้ไขปัญหา ธนาคารแห่งประเทศไทยมีการออกแนวทางนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน เพื่อยกระดับการป้องกันโดยให้ธนาคารทุกแห่ง งดส่งลิงก์ SMS ปิดกั้นคอลเซ็นเตอร์ อ้างชื่อหลอกลวง จำกัด Mobile Banking 1 บัญชี 1 ผู้ใช้งาน ในการยืนยันตัวตน โอนเงิน 50,000 ขึ้นไปต้องยืนยันตัวตน พร้อมเพิ่มมาตรการเข้มงวด ตรวจจับติดตามบัญชีต้องสงสัย

ปลายปี 2566 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ตั้งศูนย์ต่อต้านอาชญากรรมออนไลน์ (Anti Online Scam Operation Center: AOC) สายด่วน 1441 เปิดให้บริการเพื่อปฏิบัติการพิเศษเฉพาะกิจให้บริการแบบศูนย์รวม One Stop Service รับแจ้งและติดตามช่วยเหลือผู้เสียหาย โดยหลังจัดตั้งศูนย์เพียง 1 เดือนสามารถอายัดบัญชีธนาคารได้ถึง 7,996 บัญชี เป็นบัญชีคดีหลอกลวงให้ซื้อสินค้าสูงที่สุดถึง ร้อยละ 44.8 รองลงมาหลอกลวงหารายได้พิเศษ ร้อยละ 13.2 หลอกลวงให้ลงทุน ร้อยละ 8.6 หลอกให้กู้เงิน ร้อยละ 7.8 และแก๊งคอลเซ็นเตอร์ ร้อยละ 7.2 ทั้งนี้ แม้ว่าแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงินของธนาคารแห่งประเทศไทย จะกำหนดให้เยียวยาความเสียหายให้แก่ผู้บริโภคกรณีภัยทางการเงินไม่ได้เกิดจากความผิดพลาดหรือบกพร่องของธนาคาร แต่การเยียวยาก็ยังไม่เป็นไปตามที่กำหนด และผู้บริโภคยังคงต้องฟ้องดำเนินคดีกับธนาคารเพื่อเรียกเงินคืนเอง

สภาผู้บริโภคจึงเสนอให้สถาบันการเงินเปิดเผยบัญชีมิจฉาชีพ (บัญชีม้า) และบัญชีแบล็คลิส ให้ผู้บริโภคทราบ และมีระบบการแจ้งเตือนหมายเลขบัญชีที่ต้องสงสัยที่ถูกนำไปใช้ในการกระทำความผิด (Hight Risk) เพื่อแจ้งเตือนก่อนจะมีการโอนเงินไปยังบัญชีมิจฉาชีพเหล่านั้น

นอกจากนี้ ยังเสนอให้ธนาคารแห่งประเทศไทยและสมาคมธนาคารไทย กำหนดหลักเกณฑ์ให้สถาบันการเงินตั้งกองทุนหรือทำหลักประกันคุ้มครองความเสียหาย ในการฝากเงินกับสถาบันการเงินกรณีเกิดภัยทุจริตทางการเงิน เพื่อสร้างความเชื่อมั่นในการดูแลรักษาเงินของผู้บริโภค และสามารถเยียวยาความเสียหายของผู้บริโภคที่จะเกิดขึ้นทันที

สำนักวิชาการ
สำนักงานเลขาธิการสภาผู้แทนราษฎร
โทร. 0 2242 5900 ต่อ 5730, 5740, 5750
Bureau of Academic Services
The Secretariat of the House of Representatives
Tel. 0 2242 5900 ext. 5730, 5740, 5750

พิมพ์ที่ : สำนักการพิมพ์ สำนักงานเลขาธิการสภาผู้แทนราษฎร