

ปัญหากฎหมายเกี่ยวกับความรับผิดของสถาบันการเงินจากอาชญากรรมทางเทคโนโลยี¹

วีรศ หงษ์ทองคำ²

จากการศึกษาปัญหากฎหมายเกี่ยวกับความรับผิดของสถาบันการเงินจากอาชญากรรมทางเทคโนโลยี มีวัตถุประสงค์เพื่อศึกษาประวัติ ความเป็นมา แนวคิด และทฤษฎีเกี่ยวกับอาชญากรรมทางเทคโนโลยีของสถาบันการเงิน ซึ่งทำให้ผู้ศึกษาได้รับความรู้ความเข้าใจว่า สถาบันการเงินได้นำเทคโนโลยีมาใช้ในการให้บริการ เพื่อตอบสนองความต้องการของลูกค้าและเพิ่มประสิทธิภาพในการดำเนินงาน อย่างไรก็ตาม การพึ่งพาเทคโนโลยีที่มากขึ้นได้นำมาซึ่งความเสี่ยงและภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นเช่นกัน อาชญากรรมทางเทคโนโลยีได้กลายเป็นปัญหาสำคัญที่สถาบันการเงินต้องเผชิญในปัจจุบัน การเปลี่ยนแปลงจากระบบการเงินแบบดั้งเดิมสู่ระบบดิจิทัล การเพิ่มขึ้นของการให้บริการธนาคารออนไลน์และแอปพลิเคชันมือถือ (Mobile Banking) ตลอดจนการเกิดขึ้นของสกุลเงินดิจิทัลและเทคโนโลยี Blockchain ได้เปิดโอกาสให้อาชญากรพัฒนาวิธีการ โจมตีที่ซับซ้อนมากขึ้น ส่งผลให้ภัยคุกคามทางไซเบอร์เพิ่มขึ้นอย่างมีนัยสำคัญ สร้างความเสียหายให้แก่ผู้ประกอบการในธุรกิจต่าง ๆ ตลอดจนประชาชนบุคคลทั่วไปที่เป็นลูกค้าของธนาคาร ผลกระทบของอาชญากรรมทางเทคโนโลยีส่งต่อความสัมพันธ์ระหว่างสถาบันการเงินกับลูกค้า รวมถึงความเสียหายทางการเงินโดยตรง ต้นทุนในการป้องกันและรับมือที่กับอาชญากรรมทางเทคโนโลยีของสถาบันการเงินสูงขึ้น ตลอดจนผลกระทบต่อชื่อเสียงและความเชื่อมั่นของลูกค้า จนปัจจุบันมีการใช้วิธีการทางเทคโนโลยีหลอกลวงประชาชนทั่วไปผ่านอุปกรณ์เทคโนโลยีต่าง ๆ จนทำให้ประชาชนสูญเสียทรัพย์สินเป็นจำนวนมากและผู้หลอกลวงได้โอนทรัพย์สินที่ได้จากการกระทำความผิดดังกล่าวผ่านบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์หรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลอื่นต่อไปเป็นทอด ๆ อย่างรวดเร็ว เพื่อปกปิดหรืออำพรางการกระทำความผิด ซึ่งแต่ละวันประชาชนผู้สุจริตถูกหลอกลวงจำนวนมากและมีมูลค่าความเสียหายสูงมาก ส่งผลกระทบต่อประชาชนในวงกว้างและเป็นอันตรายร้ายแรงต่อระบบเศรษฐกิจของประเทศ การป้องกันการเกิดปัญหาอาชญากรรมทางเทคโนโลยีที่ดีแนวทางหนึ่ง คือการให้ความรู้ความเข้าใจเกี่ยวกับอาชญากรรมทางเทคโนโลยี ตลอดจนกฎหมายและบทลงโทษอาชญากรรมทางเทคโนโลยี เพื่อให้เกิดการป้องกันอาชญากรรมทางเทคโนโลยีที่เหมาะสม

¹บทความนี้เรียบเรียงจากการค้นคว้าอิสระ เรื่อง ปัญหากฎหมายเกี่ยวกับความรับผิดของสถาบันการเงินจากอาชญากรรมทางเทคโนโลยี โดยมีอาจารย์ที่ปรึกษา คือ รองศาสตราจารย์ ดร.กัลยา ตันศิริ และคณะกรรมการสอบ คือ รองศาสตราจารย์ประเสริฐ ตันศิริ และรองศาสตราจารย์สุรินทร์ รัตนวราห

²นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต (วิทยาเขตบางนา) คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

จากการศึกษาทำให้ทราบว่าปัญหากฎหมายเกี่ยวกับความรับผิดชอบของสถาบันการเงินจากอาชญากรรมทางเทคโนโลยี ที่สืบเนื่องมาจากพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ยังไม่ชัดเจนในการบังคับใช้กฎหมายให้บรรลุวัตถุประสงค์ ดังนี้

ปัญหาประการที่หนึ่ง คือ ปัญหาเกี่ยวกับการไม่มีบทบัญญัติให้สถาบันการเงินต้องรับผิดชอบอาชญากรรมทางเทคโนโลยี ในกรณีการถูกหลอกลวงทางเทคโนโลยี ตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ยังไม่ครอบคลุมถึงการบังคับให้สถาบันการเงินรับผิดชอบต่อการสูญเสียที่เกิดจากการถูกหลอกลวงให้ออนเงินด้วยความสมัครใจหรือไม่ได้สมัครใจ ซึ่งทำให้ผู้เสียหายต้องดำเนินการฟ้องร้องเพื่อเรียกร้องค่าเสียหายเอง ในขณะที่ประเทศอังกฤษมีมาตรการคุ้มครองลูกค้าจากการถูกหลอกลวงทางการเงินที่เข้มงวด เช่น การบังคับให้สถาบันการเงินต้องคืนเงินให้แก่ผู้เสียหายทั้งในกรณีที่ผู้เสียหายทำธุรกรรมออนไลน์ด้วยความสมัครใจและที่ไม่ได้เกิดจากความสมัครใจ ส่วนประเทศสิงคโปร์ก็มีมาตรการคุ้มครองลูกค้าจากการฉ้อโกงและธุรกรรมที่ไม่ได้รับอนุญาตกำหนดให้สถาบันการเงินต้องแจ้งเตือนเจ้าของบัญชีโดยการส่ง SMS หากมีเงินโอนออกจากบัญชี และถ้าไม่มีข้อความ SMS แจ้งเตือน ธนาคารต้องรับผิดชอบต่อเงินคืนตามจำนวน ทั้งนี้ การทำธุรกรรมทางการเงินที่ไม่ได้รับอนุญาตจะต้องไม่ได้เกิดจากความประมาทของผู้เสียหายเอง

ปัญหาประการที่สอง คือ ปัญหาเกี่ยวกับการระงับการทำธุรกรรมทางการเงินของสถาบันการเงิน แม้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 6 และมาตรา 7 จะให้อำนาจกับสถาบันการเงินในการระงับการทำธุรกรรมทางการเงินเมื่อพบเหตุอันควรสงสัยเกี่ยวกับการกระทำผิดทางเทคโนโลยี หรือเมื่อสถาบันการเงินได้รับแจ้งจากผู้เสียหาย แต่การระงับธุรกรรมในทางปฏิบัติยังคงมีข้อจำกัดในเรื่องเทคโนโลยีในการตรวจสอบธุรกรรมทางการเงินที่น่าสงสัยเข้าข่ายการฉ้อโกงทางการเงินไม่สามารถระงับได้ทั้งหมดทั้งนี้ จึงเปิดโอกาสให้มิจก้าซีฟออนไลน์ออกจากระบบได้อย่างรวดเร็ว รวมถึงข้อจำกัดขั้นตอนการปฏิบัติงานของศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (AOC) ไม่สามารถดำเนินการเองได้ ซึ่งทำหน้าที่เป็นตัวกลางในการรับแจ้งเหตุจากผู้เสียหาย และต้องแจ้งไปยังสถาบันการเงินให้เป็นผู้ดำเนินการระงับการทำธุรกรรมทางการเงิน เนื่องจากระบบงานภายในของแต่ละธนาคารแตกต่างกัน ยังไม่สามารถเชื่อมโยงกันได้ ในขณะที่ประเทศอังกฤษ สถาบันการเงินได้นำเทคโนโลยีปัญญาประดิษฐ์หรือ AI ที่ทันสมัยมาช่วยเพิ่มประสิทธิภาพ โดย AI จะวิเคราะห์พฤติกรรมการเงินของลูกค้า เพื่อตรวจจับการเคลื่อนไหวที่เข้าข่ายผิดปกติ เช่น โอนเงินไปยังบัญชีที่อาจเป็นธุรกิจหรือบุคคลปลอมหรือผิดกฎหมาย โดย AI จะตรวจสอบข้อมูลการทำธุรกรรมแบบบัญชีต่อบัญชี (Account-To-Account) และช่วยวิเคราะห์ข้อมูลสำคัญ อีกทั้งสืบค้นข้อมูลการกระทำผิดของเจ้าของบัญชี ซึ่งช่วยทำให้หลายธนาคารสามารถระงับธุรกรรมต้องสงสัยได้แบบ Real-Time ก่อนที่จะเกิดความสูญเสีย ส่วนประเทศสิงคโปร์ ศูนย์ต่อต้านขบวนการหลอกลวงเงินทางออนไลน์ The Anti-

Scam Centre (ASC) มีการใช้เทคโนโลยี "Project COMBAT" เพื่อระงับบัญชีธนาคารที่เกี่ยวข้องกับการฉ้อโกงได้อย่างรวดเร็ว โดยเป็นการให้หุ่นยนต์ส่ง SMS ไปยังผู้เสียหายเพื่อแจ้งเตือนการถูกหลอกลวง หากระบบได้ตรวจสอบพบว่ามีการทำธุรกรรมที่ผิดปกติ

ปัญหาประการที่สาม คือ ปัญหาเกี่ยวกับการแลกเปลี่ยนข้อมูลของสถาบันการเงิน โดยพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 มาตรา 4 กฎหมายยังไม่มี ความชัดเจนในเรื่องการแลกเปลี่ยนข้อมูลระหว่างสถาบันการเงิน ซึ่งธนาคารแห่งประเทศไทยเป็นส่วนหนึ่งของหน่วยงานรัฐและที่มีหน้าที่ในการกำกับดูแลธนาคารพาณิชย์ซึ่งจะต้องดำเนินการออกมาตรการกำกับดูแลให้เป็นไปตามพระราชกำหนดดังกล่าว จึงถือว่าเป็นช่องว่างในการจะบังคับใช้กฎหมายให้สมบูรณ์ ซึ่งปัจจุบันธนาคารแห่งประเทศไทยได้มีการยกระดับมาตรการจัดการภัยทุจริตทางการเงินเกี่ยวกับระบบ Central Fraud Registry (CFR) ที่เป็นระบบแลกเปลี่ยนข้อมูลเส้นทางการเงินของภาคธนาคาร เพื่อใช้ในการสืบสวนสอบสวนและอายัดบัญชีของผู้ต้องสงสัยมาใช้ระหว่างธนาคาร เพื่อดำเนินการกับบัญชีต้องสงสัยได้ครอบคลุมและรวดเร็วขึ้น รวมทั้งเป็นมาตรฐานเดียวกันนั้น แต่จะเห็นได้ว่าการแลกเปลี่ยนข้อมูลระหว่างสถาบันการเงินกับหน่วยงานที่เกี่ยวข้องยังไม่เชื่อมโยงการเป็นระบบเดียวกัน ซึ่งมีข้อจำกัดในเรื่องข้อมูลที่ใช้เป็นข้อมูลระหว่างสถาบันการเงินภายในประเทศเท่านั้น ไม่ได้รวมถึงบัญชีกระเป๋าเงินอิเล็กทรอนิกส์ (E-wallet) จากแพลตฟอร์มออนไลน์ทำให้ไม่สามารถตรวจสอบเส้นทางการเงินหากเงินออกจากบัญชีม้าไปยังบัญชีกระเป๋าเงินอิเล็กทรอนิกส์ (E-wallet) นอกจากนี้ยังไม่สามารถเชื่อมโยงข้อมูลกับสถาบันการเงินหรือหน่วยงานในต่างประเทศ จึงทำให้การดำเนินเงินจากบัญชีม้าไปบัญชีต่างประเทศไม่สามารถตรวจสอบได้เช่นกัน ในขณะที่ประเทศอังกฤษมีการเชื่อมโยงข้อมูลในภาคของธนาคารและผู้ให้บริการบัตรเครดิต ส่วนประเทศสิงคโปร์มีระบบที่เชื่อมโยงข้อมูลกับธนาคารบริษัทฟินเทค บริษัทโทรคมนาคม ตลาดออนไลน์ และหน่วยงานอื่นๆ รวมถึงศูนย์ประสานงานต่อต้านการหลอกลวงของกองกำลังตำรวจฮ่องกง และอินเตอร์โพล

ปัญหาประการที่สี่ คือ ปัญหาเกี่ยวกับบทลงโทษของสถาบันการเงินในการป้องกันและตรวจสอบบัญชีม้า ตามมาตรา 9 และมาตรา 10 ของพระราชกำหนดการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มีการกำหนดโทษสำหรับบุคคลที่เปิดบัญชีหรือให้ผู้อื่นใช้บัญชีธนาคารหรือบัตรเครดิตของตนเอง โดยรู้หรือควรรู้อย่างจะนำไปใช้ในการกระทำความผิด ซึ่งทั้งสองมาตรานี้มุ่งเน้นลงโทษผู้ที่เปิดเผย ผู้ที่ยินยอม หรือผู้เป็นธุระจัดหาใช้บัญชีม้าในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี แต่อย่างไรก็ตาม ในส่วนของสถาบันการเงินที่มีหน้าที่รับเปิดบัญชี ยังไม่ถูกกำหนดบทลงโทษทางกฎหมายอย่างชัดเจนในกรณีที่มีการอนุญาตให้เปิดบัญชีม้าโดยไม่ตั้งใจหรือด้วยความประมาท ซึ่งสถาบันการเงินในประเทศไทยมีหน้าที่ต้องมีการรู้จำลูกค้าอย่างมีประสิทธิภาพซึ่งประกอบด้วย 2 ขั้นตอนสำคัญ ได้แก่ (1) การแสดงตนของลูกค้า (Identification) และ (2) การพิสูจน์ตัวตนลูกค้า (Verification) ตรวจสอบความถูกต้อง

ความแท้จริง และ ความเป็นปัจจุบันของข้อมูลและเอกสารหลักฐานการแสดงผล รวมถึงตรวจสอบว่าบุคคลที่มาเปิดบัญชีเงินฝาก เป็นบุคคลเดียวกันกับบุคคลในเอกสารหลักฐานการแสดงผล ส่วนหนึ่งที่ทำให้เกิดบัญชีม้าเพิ่มมากขึ้นและเป็นช่องทางให้มีฉ้อฉลทางการเงินได้อย่างรวดเร็วเกิดจากมาตรการที่ไม่เข้มงวดของสถาบันการเงิน เน้นแข่งขันกันเพื่อให้บริการเกี่ยวกับระบบการเงินสามารถเปิดบัญชีธนาคารได้โดยอิสระโดยไม่มีข้อจำกัดใด ๆ ไม่มีระบบการตรวจสอบถึงความน่าเชื่อถือของผู้ขอเปิดบัญชีว่าจะเสี่ยงต่อการเป็นผู้กระทำผิด ไม่มีมาตรการคัดกรองบุคคลที่เปิดบัญชีธนาคารเพื่อป้องกันไม่ให้นำบัญชีไปใช้ในการกระทำความผิด มีระบบการทำธุรกรรมทางการเงินที่ของเจ้าของบัญชีสามารถทำธุรกรรมได้อย่างสะดวก สบาย และเร็ว ระบบตรวจสอบและควบคุมเพื่อป้องกันความผิดพลาดของผู้ใช้บริการยังไม่ดีพอ เมื่อจะมีการระงับ/ยกเลิกการทำธุรกรรม กลับมีขั้นตอนการตรวจสอบที่ใช้ระยะเวลาและไม่สอดคล้องกับการทำธุรกรรมแรกทำให้เจ้าของบัญชีสูญเสียเงินในบัญชีไป อันส่งผลให้เกิดผลกระทบต่อความเชื่อมั่นของประชาชนผู้เป็นลูกค้าและใช้บริการของธนาคาร

จากการศึกษาค้นคว้าปัญหากฎหมายเกี่ยวกับความรับผิดชอบของสถาบันการเงินจากอาชญากรรมทางเทคโนโลยี ผู้ศึกษาจึงมีข้อเสนอแนะ คือ

1. ปัญหาเกี่ยวกับการไม่มีบทบัญญัติให้สถาบันการเงินต้องรับผิดชอบจากอาชญากรรมทางเทคโนโลยี ควรจะมีการปรับปรุงบทบัญญัติทางกฎหมายให้สถาบันการเงินมีความรับผิดชอบต่อการสูญเสียที่เกิดจากการถูกหลอกลวงทางเทคโนโลยี โดยแก้ไขเพิ่มเติมพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 15 ว่า

“เมื่อเกิดความเสียหายจากการทำธุรกรรมทางการเงินอันเป็นความผิดอาชญากรรมทางเทคโนโลยีตามพระราชกำหนดฉบับนี้ โดยไม่ได้เกิดจากความประมาทของผู้เสียหาย ให้สถาบันการเงินร่วมกันรับผิดชอบใช้เงินคืนแก่ผู้เสียหายเต็มจำนวนความเสียหายที่เกิดขึ้น

หากความเสียหายที่เกิดขึ้นตามวรรคหนึ่ง เกิดจากความประมาทของผู้เสียหายเอง ให้สถาบันการเงินร่วมกันรับผิดชอบใช้เงินคืนแก่ผู้เสียหายเพียงกึ่งหนึ่งของความเสียหายที่เกิดขึ้น”

2. ปัญหาเกี่ยวกับการระงับการทำธุรกรรมทางการเงินของสถาบันการเงิน ควรจะมีการกำหนดให้สถาบันการเงินต้องพัฒนาหรือนำเทคโนโลยีเข้ามาช่วยตรวจสอบการธุรกรรมทางการเงินและระงับธุรกรรมต้องสงสัยแบบ real-time รวมถึงมาตรการหน่วงเงินก่อนโอน (Delayed Transaction) เพื่อให้สถาบันการเงินสามารถชะลอการโอนเงินจากการทำธุรกรรมทางการเงินออนไลน์ในกรณีที่มีการโอนเงินไปยังบัญชีที่ผู้เสียหายไม่เคยทำธุรกรรมมาก่อนให้ชะลอการโอนเงินไว้ 24 ชั่วโมง หรือการกำหนดให้มีการอนุญาตให้โอนเงินจากบุคคลที่ 3 (Authorized Third Party)

3. ปัญหาเกี่ยวกับการแลกเปลี่ยนข้อมูลของสถาบันการเงิน ควรจะพัฒนาระบบ Central Fraud Registry (CFR) ให้เชื่อมโยงข้อมูลจากบัญชีกระเป๋าเงินอิเล็กทรอนิกส์ (E-wallet) จากแพลตฟอร์มออนไลน์ รวมถึง

เชื่อมโยงข้อมูลกับสถาบันการเงินหรือหน่วยงานในต่างประเทศ เพื่อป้องกันการล้าเลียงเงินโอนภายนอกประเทศทำให้ยากต่อการติดตามเส้นทางการเงิน

4. ปัญหาเกี่ยวกับบทลงโทษของสถาบันการเงินในการป้องกันและตรวจสอบบัญชีม้า ควรจะมีการปรับปรุงบทบัญญัติทางกฎหมายให้สถาบันการเงินและผู้ประกอบการตามกฎหมายว่าด้วยระบบชำระเงินมีหน้าที่ตรวจสอบความถูกต้องเกี่ยวกับตัวตนของลูกค้า การตรวจสอบการเปิดบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ รวมถึงมีบทลงโทษกับสถาบันการเงิน หรือผู้ประกอบการธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงินที่ไม่ปฏิบัติตามโดยแก้ไขเพิ่มเติมพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 10 ทวิ ว่า

“สถาบันการเงิน หรือผู้ประกอบการตามกฎหมายว่าด้วยระบบการชำระเงินใด ไม่ได้มีการตรวจสอบการเปิดบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ และบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ถูกนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ต้องระวางโทษปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท”

เอกสารอ้างอิง

เดชา อัสวสิทธิถาวร. เทคโนโลยีสารสนเทศเบื้องต้น. พิมพ์ครั้งที่ 6 (กรุงเทพฯ: วังอักษร, 2552).

สาวตรี สุขศรี. กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์. พิมพ์ครั้งที่ 2 (กรุงเทพฯ:

โครงการตำราและเอกสารประกอบการสอนคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2563).

วสุธิดา นุริตมนต์. “อิทธิพลของการยอมรับเทคโนโลยีที่มีต่อพฤติกรรมการใช้บริการธุรกรรมทางการเงินผ่านแอปพลิเคชันบนโทรศัพท์เคลื่อนที่.” วารสารสหวิทยาการวิจัย 2562, ฉบับที่ 1 (มิถุนายน 2562): หน้า 189-199.

ณัฐวุฒิ ไวทย์รุ่งโรจน์. “มาตรการทางกฎหมายของสถาบันการเงินเพื่อบรรเทาความเสียหายจากการหลอกลวงให้โอนเงินทางโทรศัพท์.” เอกัตศึกษา, จุฬาลงกรณ์ มหาวิทยาลัย, 2560.

พงศกร เสี่ยงสุข. “ความรับผิดชอบทางแพ่งของธนาคารพาณิชย์และธนาคารแห่งประเทศไทย : ศึกษากรณีเงินฝากสูญหาย.” สารนิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ ปรีดี พนมยงค์, มหาวิทยาลัยธุรกิจบัณฑิต, 2566