ปกิณกะกฎหมาย (Legal Miscellaneous)

ความรับผิดชอบของธนาคารกรณีการหลอกลวงให้ทำธุรกรรมทางการเงินออนไลน์

The Responsibility of Banks in the Case of Online Financial Fraud

สุวลักษณ์ ขันธ์ปรึกษา[*]
อาจารย์ประจำสาขาวิชากฎหมายแพ่งและธุรกิจ
สำนักวิชานิติศาสตร์ มหาวิทยาลัยแม่ฟ้าหลวง
Suwalak Khanpruksa
Lecturer in Civil and Business Law,
School of Law, Mae Fah Luang University

วันที่รับบทความ 24 มิถุนายน 2568; วันที่แก้ไขบทความ 4 กรกฎาคม 2568; วันที่ตอบรับบทความ 7 กรกฎาคม 2568

[*] นิติศาสตรบัณฑิต สาขากฎหมายพาณิชย์และธุรกิจ มหาวิทยาลัยธรรมศาสตร์, นิติศาสตรมหาบัณฑิต สาขากฎหมายเอกชน มหาวิทยาลัยธรรมศาสตร์, นิติศาสตรมหาบัณฑิต สาขากฎหมายเปรียบเทียบ มหาวิทยาลัยนาโกย่า ประเทศญี่ปุ่น, อยู่ในระหว่างเขียนวิทยานิพนธ์ในหลักสูตรนิติศาสตรดุษฎีบัณฑิต สาขากฎหมายเปรียบเทียบ มหาวิทยาลัยนาโกย่า ประเทศญี่ปุ่น; อีเมลติดต่อ suwalak.kha@mfu.ac.th

บทคัดย่อ

บทความนี้มีวัตถุประสงค์เพื่อศึกษาความรับผิดชอบของธนาคารกรณีการหลอกลวงให้ทำธุรกรรมทางการเงินออนไลน์ โดยประเด็นปัญหาทางกฎหมายเกิดจากอาชญากรรมทางเทคโนโลยีที่สร้างความเสียหายทางการเงินแก่ประเทศไทยเป็นมูลค่ามหาศาล และรูปแบบอาชญากรรมที่เกิดขึ้นเกี่ยวข้องโดยตรงกับความเสียหายทางการเงินที่อยู่ในความรับผิดชอบของธนาคาร ผลการศึกษาพบว่า ภัยทางการเงินแบ่งออกเป็น 2 ประเภท ประเภทแรก การสวมรอยทำธุรกรรมแทนผู้ใช้บริการทางการเงิน (Unauthorized Payment Fraud) และประเภทที่สอง การหลอกลวงให้ผู้ใช้บริการทางการเงินทำธุรกรรมด้วยตนเองโดยความสมัครใจ (Authorized Payment Fraud) สำหรับภัยทางการเงินประเภทแรก จากแนวคำพิพากษาของศาลชี้ว่า ความแตกต่างของ “ความรับผิดชอบของธนาคาร” กรณีมิจฉาชีพสวมรอยทำธุรกรรมแทนผู้ใช้บริการทางการเงินใน “แอปพลิเคชันบัญชีเงินฝาก” กับกรณีสวมรอยทำธุรกรรมจาก “แอปพลิเคชันบัตรเครดิต” คือ กรณีสวมรอยทำธุรกรรมในแอปพลิเคชันบัญชีเงินฝากเจ้าของบัญชีและธนาคารต้องร่วมกันรับผิดชอบคนละครึ่ง ส่วนกรณีสวมรอยทำธุรกรรมจากแอปพลิเคชันบัตรเครดิตเป็นความรับผิดชอบของธนาคารแต่เพียงผู้เดียวต่อความเสียหายทั้งหมด ส่วนภัยทางการเงินประเภทที่สองยังไม่มีแนวคำพิพากษาที่วินิจฉัยในประเด็นความรับผิดชอบของธนาคาร แต่ได้มีการประกาศใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาเพื่อแก้ปัญหาอย่างฉุกเฉินเร่งด่วน โดยมุ่งคุ้มครองประชาชนผู้สุจริตซึ่งถูกหลอกลวงจนสูญเสียไปซึ่งทรัพย์สิน ผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ และในพระราชกำหนดที่ได้แก้ไขเพิ่มเติมใหม่ล่าสุดในปี พ.ศ. 2568 ได้มีการวางหลักให้สถาบันการเงินร่วมรับผิดชอบในความเสียหายที่เกิดจากอาชญากรรมทางเทคโนโลยี (Shared Responsibility)

คำสำคัญ: อาชญากรรมทางเทคโนโลยี; คำพิพากษา; ความรับผิดชอบของธนาคาร; การสวมรอยทำธุรกรรมทางการเงิน; การหลอกลวงให้ทำธุรกรรมทางการเงินด้วยความสมัครใจ

Abstract

This article aims to study the responsibility of banks in cases of fraud involving online financial transactions. The legal issues arise from cybercrime, which has caused significant financial detriment to Thailand. The nature of these crimes is directly related to financial losses for which banks may be held responsible. The study discovers that financial threats can be categorized into two types. The first type is "Unauthorised Payment Fraud," in which transactions are carried out by impersonating the financial service provider. The second type is "Authorized Payment Fraud," in which the financial service user is deceived into willingly conducting the transaction themselves. For the first type of financial threat, court rulings indicate a distinction in the "liability of banks" between two scenarios involving unauthorized withdrawals by fraudsters through mobile applications. In cases of unauthorized withdrawals from a "deposit account application," both the account holder and the bank are held jointly liable, each responsible for half of the damages. In cases of unauthorized withdrawals from a "credit card application," the bank alone is fully liable and must bear the entire loss. As for the second type of financial threat, there are currently no relevant court precedents that address the issue of the bank's liability. However, the government has enacted the Emergency Decree on Measures for the Prevention and Suppression of Technological Crimes B.E. 2566 (2023) as an urgent response to address the issue. The Emergency Decree intends to protect innocent citizens who are deceived by losing their assets through mobile phones or electronic means. In the most recent amendment to the Emergency Decree in 2025, a new principle has been established, requiring

financial institutions to share responsibility for damage resulting from technology-related crimes.

Keywords: Technological Crimes; Judgement; Responsibility of Banks; Unauthorized Payment Fraud; Authorized Payment Fraud

1. บทนำ

อาชญากรรมทางเทคโนโลยีสร้างความเสียหายทางการเงินแก่ประเทศไทยเป็นมูลค่ามหาศาล จากข้อมูลการฉ้อโกงและหลอกลวงประชาชนผ่านทางสื่อสังคมออนไลน์ พบว่ามีประชาชนไทยถูกหลอกลวง ได้รับความเดือดร้อน และสูญเสียทรัพย์สินเป็นจำนวนมาก จากข้อมูลของกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี สถิติความเสียหายสะสมตั้งแต่วันที่ 1 มกราคม พ.ศ. 2568 - วันที่ 3 กรกฎาคม พ.ศ. 2568 ในช่วงเวลาเพียง 6 เดือน มีจำนวนคดีออนไลน์ทั้งสิ้น 170,385 เรื่อง คิดเป็นมูลค่าความเสียหายรวมประมาณ 14,390 ล้านบาท[1] และมีแนวโน้มที่การกระทำความผิดดังกล่าวจะขยายตัว ก่อให้เกิดผลร้าย และเป็นอันตรายอย่างร้ายแรงต่อระบบเศรษฐกิจของประเทศ ธนาคารแห่งประเทศไทยได้แบ่งภัยทางการเงินออกเป็น 2 ประเภทใหญ่ ๆ คือ ประเภทแรก การสวมรอยทำธุรกรรมแทนผู้ใช้บริการทางการเงิน (Unauthorized Payment Fraud) หรือที่รู้จักเป็นการทั่วไปโดยไม่เป็นทางการว่า “แอปพลิเคชัน (แอปฯ) ดูดเงิน”[2] โดยที่เหยื่อไม่ได้สมัครใจโอนเงินด้วยตนเอง และประเภทที่สอง การหลอกลวงให้ผู้ใช้บริการทางการเงินทำธุรกรรมด้วยตนเองโดยความสมัครใจ (Authorized Payment Fraud) ซึ่งในปี พ.ศ. 2568 นี้ ธนาคารแห่งประเทศไทยได้มีความพยายามที่จะแก้ไขปัญหาแอปฯ ดูดเงินด้วยการออกประกาศว่าด้วยมาตรฐานเกี่ยวกับ “Mobile Banking Security (MBS)”[3] โดยได้มีการวางมาตรการ อาทิ ให้สถาบันการเงินงดส่ง SMS หรืออีเมลที่มีลิงก์แนบ ต้องมี

---

[1] กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี, **สถิติความเสียหายสะสม ตั้งแต่วันที่ 1 มกราคม 2568 ถึง วันที่ 3 กรกฎาคม 2568** [ออนไลน์], 4 กรกฎาคม 2568. แหล่งที่มา: https://www.thaipoliceonline.go.th

[2] ผู้เขียนตั้งใจใช้คำว่า “แอปฯ ดูดเงิน” ในบทความปกิณกะกฎหมายเรื่องนี้ เพื่อให้ง่ายต่อการทำความเข้าใจของบุคคลทั่วไป เนื่องจากเป็นคำที่ใช้อย่างแพร่หลาย แม้ว่าคำดังกล่าวจะไม่ใช่คำศัพท์ทางวิชาการ

[3] ประกาศธนาคารแห่งประเทศไทย ที่ 4/2568 เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงิน ซึ่งได้ประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 142 ตอนพิเศษ 55 ง ลงวันที่ 7 กุมภาพันธ์ 2568 มีผลบังคับใช้เมื่อพ้นกำหนด 30 วัน นับแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

การสแกนใบหน้าเพื่อยืนยันตัวตนผู้ใช้บริการทางการเงินในการทำธุรกรรมผ่านบริการ Mobile Banking สำหรับการโอนเงินเกิน 50,000 บาท/ครั้ง หรือเกิน 200,000 บาท/วัน รวมถึงจำกัดให้ผู้ใช้บริการทางการเงิน 1 คน มีเพียง 1 บัญชี Mobile Banking และให้ใช้งานได้เพียงอุปกรณ์เดียวเท่านั้น มาตรการ MBS ช่วยให้ภัยทุจริตจากแอปฯ ดูดเงินลดลงอย่างมากจนแทบไม่เหลือภัยจากแอปฯ ดูดเงินในปัจจุบัน ขณะที่การถูกหลอกให้โอนเงินเองโดยสมัครใจยังคงมีความเสียหายประมาณ 5,000 ล้านบาท ในช่วงไตรมาสที่ 1 ของปี พ.ศ. 2568[4] ผู้เขียนแบ่งหัวข้อการอธิบายความรับผิดชอบของธนาคารต่อกรณีการหลอกลวงให้ทำธุรกรรมทางการเงินออนไลน์ตามประเภทของภัยทางการเงิน 2 ประเภท ดังนี้

2. ความรับผิดชอบของธนาคารกรณี “การสวมรอยทำธุรกรรมแทนผู้ใช้บริการทางการเงิน (Unauthorized Payment Fraud)”

จากการศึกษาพบว่าภัยทางการเงินประเภทนี้มีแนวคำพิพากษาของศาลที่เกี่ยวข้องกับ “ความรับผิดชอบของธนาคาร” กรณีมิจฉาชีพสวมรอยทำธุรกรรมแทนผู้ใช้บริการทางการเงินในแอปฯ บัญชีเงินฝาก และกรณีมิจฉาชีพสวมรอยทำธุรกรรมในแอปฯ บัตรเครดิต ซึ่งศาลพิพากษาให้ธนาคารมีความรับผิดชอบที่แตกต่างกัน มีสาระสำคัญดังต่อไปนี้

2.1 แนวคำพิพากษาของศาลว่าด้วยความรับผิดชอบของธนาคารกรณีแอปพลิเคชันบัญชีเงินฝาก

กรณีนี้ ได้มีแนวคำพิพากษาศาลฎีกาเกี่ยวกับความรับผิดของธนาคารกรณีถูกมิจฉาชีพลักลอบโอนเงินใน “แอปฯ บัญชีเงินฝาก” ของธนาคารผ่านเครือข่ายอินเทอร์เน็ต โดยคำพิพากษาศาลฎีกาที่ 6233/2564 มีข้อเท็จจริงว่า เหตุการณ์เกิดขึ้นในช่วงกลางดึกของวันที่ 7-8 กรกฎาคม พ.ศ. 2560 รูปแบบการหลอกลวงมีลักษณะเป็นการหลอกให้

[4] พรเพ็ญ สดศรีชัย, **ว่าด้วยการ “ร่วมรับผิดชอบ” ความเสียหายจากภัยทางการเงิน** [ออนไลน์], 19 มิถุนายน 2568. แหล่งที่มา: https://www.bot.or.th/th/research-and-publications/articles-and-publications/articles/article-20250513.html

โจทก์คลิกลิงก์ที่ส่งมาทางอีเมลซึ่งเชื่อมต่อไปยังเว็บไซต์ทำที่เลียนแบบธนาคารจำเลย (Phishing Email) เพื่อลวงให้โจทก์ ผู้เสียหาย กรอกชื่อผู้ใช้ (Username) รหัสผ่าน (Password) และหมายเลข OTP (One Time Password) ในเว็บไซต์ปลอมดังกล่าว เป็นเหตุให้มิจฉาชีพสามารถนำชื่อผู้ใช้ รหัสผ่าน และหมายเลข OTP ของโจทก์ไปสมัครใช้บริการแอปพลิเคชันของธนาคารในสมาร์ทโฟนได้สำเร็จ และมีการโอนเงินจากบัญชีเงินฝากของโจทก์ไปยังบัญชีอื่นจำนวน 3 บัญชี รวม 12 ครั้ง เป็นเงินทั้งหมด 1,099,999 บาท โจทก์จึงฟ้องให้ธนาคารรับผิดในเงินจำนวนดังกล่าว ศาลฎีกาได้วินิจฉัยความรับผิดของธนาคารไว้ สรุปได้ว่า ธนาคารจำเลยประกอบกิจการธนาคารพาณิชย์ จึง “เป็นผู้รับฝาก” ซึ่งเป็นผู้มีวิชาชีพเฉพาะกิจการค้าขายหรืออาชีวะ จำต้องใช้ความระมัดระวังและใช้ฝีมือเท่าที่เป็นธรรมดาจะต้องใช้และสมควรจะต้องใช้ในกิจการค้าขายหรืออาชีวะอย่างนั้น ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 659 วรรคสาม[5] การโอนเงินที่เป็นการโอนจำนวนย่อยหลายครั้งติดต่อกันในช่วงเวลาเดียวกันในเวลากลางคืน จากบัญชีเงินฝากของโจทก์ไปยังบัญชีเงินฝากของบุคคลอื่นโดยเป็นบัญชีเดียวกันหรือชื่อบัญชีเดียวกัน ย่อมเป็นพฤติกรรมในการทำธุรกรรมทางการเงินที่ผิดปกติ จำเลยซึ่งเป็นผู้มีวิชาชีพเฉพาะกิจการค้าขายหรืออาชีวะต้องทราบถึงวิธีการดังกล่าวและย่อมสังเกตได้ว่าเป็นเรื่องผิดปกติและอาจเป็นการกระทำของมิจฉาชีพผู้ประกอบอาชญากรรมทางอิเล็กทรอนิกส์ จำเลยจึงควรมีมาตรการที่เหมาะสมในการป้องกันการกระทำธุรกรรมทางการเงินโดยไม่ชอบดังกล่าวด้วย

---

[5] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 659 บัญญัติว่า “ถ้าการรับฝากทรัพย์เป็นการทำให้เปล่าไม่มีบำเหน็จไซร้ ท่านว่าผู้รับฝากจำต้องใช้ความระมัดระวังสงวนทรัพย์สินซึ่งฝากนั้นเหมือนเช่นเคยประพฤติในกิจการของตนเอง

ถ้าการรับฝากทรัพย์นั้นมีบำเหน็จค่าฝาก ท่านว่าผู้รับฝากจำต้องใช้ความระมัดระวังและใช้ฝีมือเพื่อสงวนทรัพย์สินนั้นเหมือนเช่นวิญญูชนจะพึงประพฤติโดยพฤติการณ์ดังนั้น ทั้งนี้ ย่อมรวมทั้งการใช้ฝีมืออันพิเศษเฉพาะการในที่จะพึงใช้ฝีมือเช่นนั้นด้วย

ถ้าและผู้รับฝากเป็นผู้มีวิชาชีพเฉพาะกิจการค้าขายหรืออาชีวะอย่างหนึ่งอย่างใดก็จำต้องใช้ความระมัดระวังและใช้ฝีมือเท่าที่เป็นธรรมดาจะต้องใช้และสมควรจะต้องใช้ในกิจการค้าขายหรืออาชีวะอย่างนั้น”

แม้ธนาคารจำเลยจะเคยแจ้งเตือนลูกค้าผู้ใช้บริการต่าง ๆ ให้ระมัดระวังอีเมลหลอกลวงจากมิจฉาชีพมาก่อนแล้วก็ตาม มาตรการดังกล่าวก็เป็นข้อควรระวังในด้านของลูกค้า แต่มาตรฐานของจำเลยในการป้องกันการโอนเงินที่เป็นการทำธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ที่ไม่ชอบควรจะมีอยู่อย่างไร จำเลยควรจะป้องกันหรือระงับยับยั้งการโอนเงินที่มีความผิดปกติเมื่อมีการโอนเงินผ่านไปแล้วกี่ครั้ง และเหตุใดพนักงานของจำเลยเพิ่งจะโทรศัพท์แจ้งเตือนไปยังโจทก์หลังจากที่มีการโอนเงินครั้งที่ 12 และโอนเงินไปแล้วถึง 1,099,999 บาท ซึ่งมาตรการในการป้องกันความเสียหายที่เหมาะสมหรือสมควรนั้นอยู่ในความรู้เห็นของจำเลยฝ่ายเดียว จำเลยจึงมีภาระการพิสูจน์ในส่วนนี้ แต่จำเลยกลับแสดงให้เห็นว่าจำเลยไม่ได้มีมาตรการในการป้องกันหากเกิดการโอนเงินหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ที่ไม่ชอบในส่วนนี้เลย และไม่ปรากฏว่าจำเลยมีมาตรการในการป้องกันความเสียหายในส่วนนี้อย่างเพียงพอ นอกจากนี้ ได้ความว่าโจทก์มิใช่รายแรกที่ถูกหลอกลวงในลักษณะนี้และมีอีกหลายรายที่ถูกหลอกลวงในลักษณะเดียวกัน ย่อมแสดงให้เห็นว่าจำเลยทราบถึงพฤติกรรมการหลอกลวงและวิธีการโอนเงินโดยไม่ชอบเช่นเดียวกับคดีนี้มาก่อน ทั้งเหตุยังเกิดซ้ำ ๆ กับลูกค้าจำนวนมาก จำเลยซึ่งเป็นผู้มีวิชาชีพเฉพาะกิจการค้าขายหรืออาชีวะและในฐานะที่เป็นผู้ควบคุมระบบมีความสามารถในการตรวจสอบหรือทราบถึงความผิดปกติในการทำรายการต่าง ๆ ได้แต่เพียงฝ่ายเดียว ยิ่งต้องเพิ่มความระมัดระวังและหามาตรการในการป้องกันไม่ให้เกิดความเสียหายดังเช่นที่เกิดในคดีนี้อีก ดังนั้น จึงไม่อาจรับฟังได้ว่าจำเลยได้ใช้ความระมัดระวังและใช้ฝีมือเท่าที่เป็นธรรมดาจะต้องใช้และสมควรจะต้องใช้ในกิจการค้าขายหรืออาชีวะอย่างนั้นแล้ว จำเลยจึงต้องรับผิดคืนเงินให้ผู้เสียหาย

อย่างไรก็ตาม ในคดีนี้ศาลฎีกามองว่าโจทก์ ผู้เสียหาย มีส่วนในความผิดด้วยเช่นกัน เนื่องจากโจทก์เป็นผู้ใช้บริการธุรกรรมทางการเงินอิเล็กทรอนิกส์ผ่านทางอินเทอร์เน็ตก่อนเกิดเหตุเป็นเวลากว่า 10 ปี ทั้งตามใบแจ้งรายการบัญชีออมทรัพย์โจทก์ก็ได้ทำธุรกรรมทางการเงินอิเล็กทรอนิกส์ผ่านทางอินเทอร์เน็ตหลายครั้ง โจทก์ย่อมมีความเข้าใจในการทำธุรกรรมทางการเงินผ่านช่องทางดังกล่าวและย่อมทราบถึงคำเตือนของจำเลยตามที่ปรากฏในเว็บไซต์ของจำเลย โจทก์จึงควรมีความระมัดระวังในการตรวจสอบก่อนทำธุรกรรมดังกล่าวมากกว่าที่ปรากฏในคดีนี้ จึงถือว่าโจทก์มีส่วนทำให้เกิดความ

เสียหายด้วย พฤติกรรมของโจทก์และจำเลยจึงถือว่ามีส่วนทำให้เกิดความเสียหายในคดีนี้ไม่ยิ่งหย่อนกว่ากันและเห็นสมควรให้จำเลยต้องรับผิดชดใช้เงินให้แก่โจทก์ 550,000 บาท ซึ่งนับเป็นครึ่งหนึ่งของเงินที่ถูกโอนไป หมายความว่า กรณีมิจฉาชีพลักลอบโอนเงินในบัญชีเงินฝากของธนาคารผ่านเครือข่ายอินเทอร์เน็ตนั้น เจ้าของบัญชีและธนาคารร่วมกันรับผิดชอบคนละครึ่ง ซึ่งจะต่างจากความรับผิดของธนาคารกรณีมิจฉาชีพลักลอบดูดเงินจากแอปฯ บัตรเครดิต ผ่านเครือข่ายอินเทอร์เน็ต ซึ่งเพิ่งมีคำพิพากษาของศาลชั้นต้นในกรณีนี้เมื่อปี พ.ศ. 2567 ที่ผ่านมา

2.2 แนวคำพิพากษาของศาลว่าด้วยความรับผิดชอบของธนาคารกรณีแอปพลิเคชันบัตรเครดิต

เมื่อวันที่ 28 สิงหาคม พ.ศ. 2567 ศาลแขวงระยอง คดีหมายเลขแดงที่ ผบE 6791/2567 ได้มีคำพิพากษายกฟ้องกรณีผู้ถือบัตรเครดิตถูกมิจฉาชีพเข้าถึงแอปพลิเคชันบัตรเครดิต KTC และเบิกถอนเงินสดออกไปยังบัญชีธนาคารกรุงไทย อีกทั้งยังดูดเงินออกจากบัญชีดังกล่าว ข้อเท็จจริงฟังได้ว่า จำเลย ผู้ถือบัตรเครดิต ได้แจ้งโจทก์ บริษัท บัตรกรุงไทย จำกัด (มหาชน) ผู้ออกบัตรเครดิต ว่าถูกมิจฉาชีพซึ่งอ้างว่าเป็นเจ้าหน้าที่ที่ดินหลอกให้กดลิงก์เว็บไซต์ ดาวน์โหลดแอปพลิเคชัน และให้ทำตามขั้นตอนในแอปพลิเคชันซึ่งเป็นการกรอกข้อมูลส่วนตัวเพื่อจะชำระค่าภาษีที่อยู่อาศัยผ่านช่องทางออนไลน์ ระหว่างนั้นมิจฉาชีพได้สั่งให้มีการโอนเงินจากบัญชีบัตรเครดิตของจำเลยไปยังบัญชีเงินฝากธนาคารกรุงไทยของจำเลยซึ่งเป็นบัญชีที่จำเลยผูกไว้กับบัตรเครดิตดังกล่าว จากนั้นมิจฉาชีพได้โอนเงินจากบัญชีเงินฝากธนาคารกรุงไทยของจำเลยไปยังบัญชีอื่น จำเลยจึงได้โทรศัพท์แจ้งโจทก์และแจ้งความไว้ด้วย แต่ต่อมาจำเลยกลับถูกโจทก์ฟ้องเนื่องจากจำเลยไม่ได้ชำระค่าบริการตามรายการที่ถูกมิจฉาชีพเบิกถอนเงินจากบัญชีบัตรเครดิต ศาลแขวงระยองได้พิพากษายกฟ้องโดยสรุปสาระสำคัญของเหตุผลประกอบการวินิจฉัยได้ 4 ประการ[6] กล่าวคือ ประการแรก หลังจากเกิดเหตุ จำเลย ผู้ถือบัตรเครดิต ได้รีบแจ้ง

[6] สภาองค์กรของผู้บริโภค, **ชนะคดี! ผู้บริโภคถูกแบงก์ฟ้อง โดนหลอกดูดเงินบัตรเครดิต** [ออนไลน์], 19 มิถุนายน 2568. แหล่งที่มา: https://www.tcc.or.th/17092567_consumer-sued_news/

โจทก์ ผู้ออกบัตรเครดิต ทันที ซึ่งเป็นสิ่งยืนยันว่าผู้ถือบัตรเครดิตได้รีบดำเนินการเมื่อทราบเหตุ แต่เมื่อบริษัทผู้ออกบัตรเครดิตทราบเรื่องแล้วกลับเพียงแค่แจ้งให้ผู้ถือบัตรเครดิตไปแจ้งความกับตำรวจและไม่ได้ดำเนินการอื่นใดเพิ่มเติมเพื่อปกป้องไม่ให้เงินถูกถ่ายโอนไปยังบัญชีอื่น ๆ ต่อไป ประการที่สอง เงินที่ถูกโจรกรรมเป็นเงินของธนาคารผู้ออกบัตรเครดิตไม่ใช่เงินของผู้ถือบัตรเครดิต ประการที่สาม ธนาคารผู้ออกบัตรเครดิตเป็นผู้ประกอบธุรกิจที่ให้บริการทางการเงินและเป็นเจ้าของเงินที่ถูกมิจฉาชีพโจรกรรมไป สามารถสร้างเครือข่ายร่วมกับธนาคารหรือสถาบันการเงินอื่นเพื่อระงับหรืออายัดเงินดังกล่าวไว้ชั่วคราวเพื่อตรวจสอบได้ แต่กลับไม่รวมกลุ่มกันเพื่อยกระดับการป้องกันภัยทุจริตดังกล่าว และประการที่สี่ แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงินของธนาคารแห่งประเทศไทย ระบุถึงเรื่องการบริหารจัดการภัยทุจริตจากการทำธุรกรรมการชำระเงินผ่านบัตร โดยข้อ 3.2 กำหนดชัดเจนว่า “กรณีเหตุการณ์ทุจริตที่มีผู้ถือบัตรได้รับความเสียหายที่เกี่ยวข้องกับการทำธุรกรรมชำระเงินผ่านบัตร และมีเหตุอันเชื่อได้ว่าไม่ได้เกิดจากความผิดของผู้ถือบัตรหรือผู้ถือบัตรไม่มีส่วนเกี่ยวข้อง ผู้ให้บริการต้องเยียวยาความเสียหายให้แก่ผู้ถือบัตรอย่างครบถ้วน” ขณะที่มิจฉาชีพสั่งโอนเงินออกจากบัญชีบัตรเครดิตของจำเลย จำเลยไม่ทราบถึงการทำธุรกรรมดังกล่าว ทั้งมิใช่เป็นผู้ทำธุรกรรมการเงินดังกล่าวด้วยตนเอง ประกอบกับเงินที่โอนออกไปนั้นไม่ใช่เงินของจำเลย การที่โจทก์จะเอาสัญญาสำเร็จรูปมาอ้างว่าธุรกรรมการเงินที่เกิดขึ้นดังกล่าวถือเป็นการกระทำของจำเลยและจำเลยต้องรับผิดชำระหนี้บัตรเครดิตดังกล่าวให้แก่โจทก์ย่อมเป็นการใช้สิทธิที่ขัดต่อมาตรา 12 แห่งพระราชบัญญัติวิธีพิจารณาคดีผู้บริโภค พ.ศ. 2551 ซึ่งบัญญัติว่า “การใช้สิทธิแห่งตนก็ดี การชำระหนี้ก็ดี ผู้ประกอบธุรกิจต้องกระทำด้วยความสุจริต โดยคำนึงถึงมาตรฐานทางการค้าที่เหมาะสม ภายใต้ระบบธุรกิจที่เป็นธรรม” จึงพิพากษายกฟ้อง ดังนั้น ธนาคารผู้ออกบัตรเครดิตจึงต้องรับผิดในความเสียหายทั้งหมดที่เกิดขึ้น

คำพิพากษาศาลแขวงระยอง คดีหมายเลขแดงที่ ผบE 6791/2567 ดังกล่าวกลายเป็นบรรทัดฐานเรื่องความรับผิดของธนาคารกรณีมิจฉาชีพลักลอบดูดเงินจากแอปฯ

บัตรเครดิต ผ่านเครือข่ายอินเทอร์เน็ต โดยในเดือนกันยายน พ.ศ. 2567 ศาลแขวงเชียงใหม่ได้มีคำพิพากษายกฟ้องในกรณีที่ใกล้เคียงกัน ข้อเท็จจริงคือ จำเลย ผู้ถือบัตรเครดิต ถูกมิจฉาชีพโทรศัพท์ติดต่อมาแอบอ้างว่าเป็นเจ้าหน้าที่จากกรมที่ดิน ลวงให้เข้าเว็บไซต์กรมที่ดินปลอมและให้ดาวน์โหลดติดตั้งแอปพลิเคชันกรมที่ดินปลอม ภายหลังติดตั้งพบว่าโทรศัพท์มือถือไม่สามารถใช้งานได้ เครื่องค้าง และพบว่ามีรายการทำธุรกรรมทางการเงินที่ผิดปกติ 3 ครั้ง คือ มีการเบิกถอนเงินสดจากบัตรเครดิต ครั้งละ 40,000 บาท รวมจำนวนเงิน 120,000 บาท เข้าบัญชีจำเลย ผู้เสียหาย ที่ผูกไว้กับธนาคาร หลังจากนั้นมีการแจ้งเตือนว่ามีการโอนเงินจากบัญชีผู้เสียหายไปยังบัญชีมิจฉาชีพ จำนวนเงิน 120,000 บาท เมื่อผู้ถือบัตรเครดิตที่ได้รับความเสียหายทราบเรื่องจึงรีบแจ้งไปยังธนาคารผู้ออกบัตรเครดิตและรีบแจ้งความกับตำรวจโดยทันที แต่เมื่อเดือนเมษายน พ.ศ. 2566 กลับถูกโจทก์ธนาคารผู้ออกบัตรเครดิต ฟ้องเรียกให้ชำระเงินจำนวนทั้งสิ้น 142,000 บาท (รวมดอกเบี้ยค่าติดตามทวงถาม และค่าธรรมเนียมเบิกถอน) หลังจากได้มีการพิจารณาคดี ศาลแขวงเชียงใหม่ได้มีคำพิพากษายกฟ้อง ในเหตุผลประกอบการวินิจฉัยมีประเด็นที่น่าสนใจสามประเด็น[7] ได้แก่ หนึ่ง การแจ้งความและร้องทุกข์ของจำเลยแสดงถึงความสุจริตและการปฏิบัติตนอย่างเหมาะสมของผู้ถือบัตรเครดิต สอง บัญชีปลายทางที่มีการถูกอายัดแสดงว่าเคยมีประวัติการฉ้อโกง ซึ่งช่วยเพิ่มความเป็นธรรมให้ผู้ถือบัตรเครดิต และสาม การเบิกเงินเกิน 40,000 บาท โดยผู้ถือบัตรเครดิตไม่เคยใช้ในลักษณะนี้ ธนาคารผู้ออกบัตรเครดิตควรตรวจพบและสังเกตความผิดปกติเพื่อลดการฉ้อโกง

อีกกรณี ในวันที่ 26 กุมภาพันธ์ พ.ศ. 2568 ศาลแขวงขอนแก่นได้มีคำพิพากษายกฟ้องในคดีที่ผู้ถือบัตรเครดิตถูกดูดเงินในบัตรเครดิต โดยมิจฉาชีพอ้างตัวเป็นเจ้าหน้าที่การไฟฟ้าแจ้งให้เหยื่อเปลี่ยนมิเตอร์ไฟฟ้าเป็นระบบดิจิทัลและหลอกให้ติดตั้งแอปพลิเคชันปลอมที่สามารถเข้าควบคุมโทรศัพท์มือถือและแอปฯ บัตรเครดิตจากระยะไกลได้ ส่งผลให้มิจฉาชีพสามารถถอนเงินสดจากแอปฯ บัตรเครดิตไปโดยที่ผู้ถือบัตรเครดิตไม่รู้ตัว เมื่อ

[7] สภาองค์กรของผู้บริโภค, **ศาลเชียงใหม่ยกฟ้อง! กรณีไม่จ่ายหนี้บัตรเครดิต หลังผู้บริโภคโดนดูดเงิน** [ออนไลน์], 19 มิถุนายน 2568. แหล่งที่มา: https://www.tcc.or.th/dismiss-creditcard-fraud/

ทราบว่าถูกดูดเงิน จำเลย ผู้ถือบัตรเครดิต ได้รีบแจ้งความต่อพนักงานสอบสวนที่สถานีตำรวจภูธรเมืองขอนแก่น และติดต่อโจทก์ บริษัท บัตรกรุงไทย จำกัด (มหาชน) เพื่อยืนยันว่าตนไม่ได้เป็นผู้ทำธุรกรรมด้วยตัวเอง แต่บริษัทผู้ออกบัตรเครดิตกลับยื่นฟ้องผู้ถือบัตรเครดิตให้ชำระหนี้จำนวน 100,000 บาท พร้อมดอกเบี้ย ซึ่งศาลแขวงขอนแก่นได้มีคำพิพากษายกฟ้องโดยสรุปเหตุผลได้ว่า หลังจากเกิดเหตุผู้ถือบัตรเครดิตรีบแจ้งความที่สถานีตำรวจว่าถูกหลอกลวง เป็นการยืนยันว่าผู้เสียหายได้รีบดำเนินการเมื่อทราบเหตุ และผู้ถือบัตรเครดิตถูกขโมยรหัสลับเฉพาะบุคคล (Personal Identification Number: PIN) ผ่านเครื่องมือควบคุมโทรศัพท์เคลื่อนที่ระยะไกลโดยไม่ได้ยินยอมที่จะให้ข้อมูลนั้นกับบุคคลอื่น ศาลยังได้วินิจฉัยว่า ข้อตกลงและเงื่อนไขในคำขอเบิกสินเชื่อที่กำหนดให้ผู้ถือบัตรเครดิตต้องรับผิดชอบในธุรกรรมอิเล็กทรอนิกส์ที่มีการใช้รหัสประจำตัวของบริษัทผู้ออกบัตรเครดิตในทุกกรณี เป็นข้อตกลงและเงื่อนไขที่ทำให้ผู้ถือบัตรเครดิตเสียเปรียบเกินสมควร **“เป็นข้อสัญญาที่ไม่เป็นธรรม”** นอกจากนี้ ยังมีหลักฐานยืนยันเชื่อได้ว่าการทำธุรกรรมถอนเงินสดที่เกิดขึ้นไม่ได้เกิดขึ้นโดยที่ผู้ถือบัตรเครดิตเป็นผู้ทำรายการด้วยตัวเอง[8]

2.3 บทวิเคราะห์คำพิพากษา

จากคำพิพากษาของศาล ความแตกต่างของ “ความรับผิดชอบของธนาคาร” กรณีถูกมิจฉาชีพลักลอบดูดเงินใน “แอปฯ บัญชีเงินฝาก” กับกรณีถูกมิจฉาชีพดูดเงินจาก “แอปฯ บัตรเครดิต” คือ กรณีถูกดูดเงินจากแอปฯ บัญชีเงินฝากเจ้าของบัญชีและธนาคารต้องร่วมกันรับผิดชอบคนละครึ่ง ส่วนกรณีถูกมิจฉาชีพลักลอบดูดเงินจากแอปฯ บัตรเครดิต เป็นความรับผิดชอบของธนาคารผู้ออกบัตรเครดิตแต่เพียงผู้เดียวต่อความเสียหายทั้งหมด โดยแนวคำพิพากษากรณีลักลอบดูดเงินจากแอปฯ บัตรเครดิตทั้ง 3 คดี มีข้อเท็จจริงที่ยืนยันถึงความสุจริตของผู้เสียหายที่เมื่อทราบเหตุก็รีบติดต่อผู้ออกบัตรเครดิตและแจ้งความเพื่อดำเนินคดี ทั้งนี้ การฝากเงินในธนาคารและการใช้บัตรเครดิตมีฐานของสัญญาที่แตกต่างกัน เงินฝากในธนาคารอยู่ภายใต้หลักกฎหมายว่าด้วย **“สัญญาฝาก**

[8] สภาองค์กรของผู้บริโภค, **ศาลยกฟ้อง กรณีถูกดูดเงินในบัตรกรุงไทยฯ** [ออนไลน์], 20 มิถุนายน 2568. แหล่งที่มา: https://www.tcc.or.th/dismiss-consumer-fraud/

ทรัพย์” ซึ่งประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 672[9] วางหลักไว้ว่าผู้รับฝากเงินไม่จำเป็นต้องส่งคืนเงินตราอันเดียวกันกับที่ฝาก แต่จะต้องคืนเงินให้ครบจำนวน ส่วนสัญญาบัตรเครดิตเป็นสัญญาประเภทหนึ่งที่ไม่ได้ระบุไว้เป็นเอกเทศตามประมวลกฎหมายแพ่งและพาณิชย์ จึงนับเป็นสัญญาไม่มีชื่อที่เกิดขึ้นโดยหลักเสรีภาพในการทำสัญญา (Freedom of Contract) สัญญาบัตรเครดิตมีลักษณะเป็นสัญญาที่เกี่ยวข้องกับคู่สัญญาทั้งหมดสามฝ่าย ประกอบด้วย ผู้ออกบัตรเครดิต ผู้ถือบัตรเครดิต และร้านค้าหรือสถานบริการผู้รับบัตรเครดิต มีสาระสำคัญคือ เมื่อผู้ถือบัตรเครดิตนำบัตรเครดิตที่ออกโดยธนาคารพาณิชย์หรือสถาบันที่ประกอบธุรกิจบัตรเครดิตไปแสดงต่อร้านค้าหรือสถานบริการต่าง ๆ ที่ได้มีข้อตกลงกับผู้ออกบัตร ผู้ถือบัตรเครดิตจะสามารถใช้บัตรเครดิตนั้นซื้อสินค้าหรือบริการจากร้านค้าหรือสถานบริการต่าง ๆ นั้นได้โดยที่ผู้ถือบัตรเครดิตไม่ต้องชำระเป็นเงินสด ซึ่งร้านค้าหรือสถานบริการจะเรียกเก็บเงินจากผู้ออกบัตรเครดิต เมื่อผู้ออกบัตรเครดิตได้ชำระเงินให้แก่ร้านค้าหรือสถานบริการไปแล้ว ผู้ออกบัตรเครดิตจึงจะเรียกเก็บเงินจากผู้ถือบัตรเครดิตต่อไปในภายหลัง โดยผู้ถือบัตรเครดิตต้องชำระเงินคืนให้แก่ผู้ออกบัตรเครดิตภายในกำหนดระยะเวลาที่ได้ตกลงกันไว้[10] แม้ว่าความรับผิดชอบของธนาคารกรณีถูกมิจฉาชีพลักลอบดูดเงินในแอปฯ บัญชีเงินฝาก กับกรณีถูกมิจฉาชีพดูดเงินจากแอปฯ บัตรเครดิต จะแตกต่างกัน แต่ความรับผิดของธนาคารทั้ง 2 กรณีนี้ ต่างก็เกิดจากการสวมรอยทำธุรกรรมแทนผู้ใช้บริการทางการเงิน (Unauthorized Payment Fraud) ที่เหยื่อหรือผู้เสียหายไม่ได้สมัครใจโอนเงินด้วยตนเองเหมือนกัน

---

[9] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 672 บัญญัติว่า “ถ้าฝากเงิน ท่านให้สันนิษฐานไว้ก่อนว่า ผู้รับฝากไม่พึงต้องส่งคืนเป็นเงินทองตราอันเดียวกันกับที่ฝาก แต่จะต้องคืนเงินให้ครบจำนวน

อนึ่ง ผู้รับฝากจะเอาเงินซึ่งฝากนั้นออกใช้ก็ได้ แต่หากจำต้องคืนเงินให้ครบจำนวนเท่านั้น แม้ว่าเงินซึ่งฝากนั้นจะได้สูญหายไปด้วยเหตุสุดวิสัยก็ตาม ผู้รับฝากก็จำต้องคืนเงินเป็นจำนวนดังว่านั้น”

[10] มนูญธรรม ปรีชาไว, **ความรับผิดทางแพ่งจากการใช้บัตรเครดิต (กรณีมีเซลสลิป)**, วารสารกระบวนการยุติธรรม, ปีที่ 5 (พฤษภาคม-สิงหาคม 2555), หน้า 29.

3. ความรับผิดชอบของธนาคารกรณี “การหลอกลวงให้ผู้ใช้บริการทางการเงินทำธุรกรรมด้วยตนเองโดยความสมัครใจ (Authorized Payment Fraud)”

ในขณะที่ภัยทุจริตจากแอปฯ ดูดเงินกำลังลดลงเรื่อย ๆ แต่ภัยทางการเงินอีกประเภทหนึ่ง ซึ่งก็คือ “การหลอกลวงให้ผู้ใช้บริการทางการเงินทำธุรกรรมด้วยตนเองโดยความสมัครใจ” ยังคงมีมูลค่าความเสียหายสูงมาก และมีเหยื่อหรือผู้เสียหายเป็นข่าวสะเทือนใจผ่านสื่อให้เห็นอยู่เสมอ โดยเฉพาะการถูกหลอกให้โอนเงินโดย “แก๊งคอลเซ็นเตอร์” กรณีโดนหลอกให้โอนเงินโดยสมัครใจนี้แม้จะยังไม่มีแนวคำพิพากษาที่วินิจฉัยในประเด็นความรับผิดชอบของธนาคาร แต่ได้มีการประกาศใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาเพื่อแก้ปัญหาอย่างฉุกเฉินเร่งด่วน เหตุผลและความจำเป็นในการตราพระราชกำหนดฉบับนี้มีวัตถุประสงค์เพื่อมุ่งคุ้มครองประชาชนผู้สุจริตซึ่งถูกหลอกลวงจนสูญเสียไปซึ่งทรัพย์สิน ผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ พระราชกำหนดฉบับนี้มีสาระสำคัญ 4 ประการ[11] ได้แก่ ประการแรก กำหนดให้สถาบันการเงิน ผู้ให้บริการโทรคมนาคม ผู้ประกอบธุรกิจที่เกี่ยวข้อง และหน่วยงานรัฐบางหน่วยงาน ได้แก่ สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ และสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) มีอำนาจเข้าถึงและแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าผ่านระบบการแลกเปลี่ยนข้อมูล โดยสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) เป็นหน่วยงานจัดทำระบบฐานข้อมูลกลางเท่าที่จำเป็น ประการที่สอง กำหนดให้สถาบันการเงินหรือผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงินมีหน้าที่ระงับยับยั้งธุรกรรมต้องสงสัยหรือเกี่ยวข้องกับการกระทำความผิดและนำข้อมูลเข้าสู่ระบบการแลกเปลี่ยนข้อมูลเพื่อให้ผู้รับโอนทุกทอดทราบและระงับการทำธุรกรรมนั้นทันที ประการที่สาม ประชาชนที่ถูกหลอกลวงหรือสงสัยว่าตกเป็นเหยื่อของมิจฉาชีพสามารถแจ้งธนาคาร

[11] ฝ่ายนวัตกรรมการเรียนรู้และสื่อสารองค์กร คณะนิติศาสตร์ มหาวิทยาลัยพะเยา, **ทำความรู้จัก พ.ร.ก. ป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และ (ร่าง) พรก. ไซเบอร์** [ออนไลน์], 20 มิถุนายน 2568. แหล่งที่มา: https://www.up.ac.th/NewsReadBlog2.aspx?itemID=33995

หรือสถาบันการเงินผ่านศูนย์รับแจ้งเหตุภัยทางการเงินเพื่อยับยั้งการทำธุรกรรมการเงินที่ต้องสงสัยชั่วคราวได้ และสามารถแจ้งความร้องทุกข์ต่อพนักงานสอบสวน ณ สถานีตำรวจได้ทุกท้องที่ทั่วประเทศ หรือแจ้งต่อพนักงานสอบสวนของกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) ที่รู้จักในชื่อ “กองบัญชาการตำรวจไซเบอร์” หรือแจ้งผ่านระบบการรับแจ้งความออนไลน์ www.thaipoliceonline.com ภายในระยะเวลา 72 ชั่วโมง เพื่อให้พนักงานสอบสวนดำเนินการติดต่อให้สถาบันการเงินอายัดเงินในบัญชีภายใน 7 วัน นับตั้งแต่วันที่ได้รับคำร้องทุกข์ และประการที่สี่ มีการกำหนดความผิดและโทษทางอาญาสำหรับการเปิด เป็นธุระจัดหา โฆษณา หรือไขข่าวเพื่อให้มีการซื้อหรือขาย “บัญชีม้า” และ “ซิมม้า” เพื่อนำไปใช้กระทำความผิด โดยผู้กระทำความผิดดังกล่าวอาจต้องระวางโทษจำคุกตั้งแต่ 2-5 ปี หรือปรับตั้งแต่ 200,000-500,000 บาท หรือทั้งจำทั้งปรับ แต่ทั้งนี้ ยังไม่มีการกำหนดความรับผิดสำหรับผู้ที่ “ใช้หรือถือครอง” บัญชีม้าหรือซิมม้าที่แท้จริง[12]

เมื่อไม่นานมานี้ได้มีการประกาศใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 13 เมษายน พ.ศ. 2568 เพื่อเป็นการแก้ไขเพิ่มเติมพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 กฎหมายใหม่ได้เพิ่มเติมนิยามของคำว่า “ผู้ประกอบธุรกิจ” ให้หมายความรวมถึง “กระเป๋าสินทรัพย์ดิจิทัล” และ “บัญชีเงินอิเล็กทรอนิกส์” มีการกำหนดให้สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) เป็นหน่วยงานในการกำกับดูแลการประกอบธุรกิจสินทรัพย์ดิจิทัล เปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับเลขที่กระเป๋าสินทรัพย์ดิจิทัล รวมถึงการแจ้งรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี กฎหมายยังกำหนดให้มีการตรวจสอบเพื่อคัดกรองเนื้อหาการ

[12] ศิรวิษ สุขชัย และปริญญา ศรีเกตุ, **มาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี: ศึกษากรณีการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้า**, วารสารนวัตกรรมการศึกษาและการวิจัย, ปีที่ 8 ฉบับที่ 4 (ตุลาคม-ธันวาคม 2567), หน้า 1876.

บริการ SMS ที่อาจเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ให้อำนาจสำนักงาน กสทช. สั่งให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้อง ระงับการให้บริการโทรคมนาคมเมื่อปรากฏพยานหลักฐานอันควรเชื่อได้ว่ามีการใช้บริการโทรคมนาคมเพื่อกระทำความผิดอาชญากรรมทางเทคโนโลยี ให้อำนาจสำนักงาน ปปง. ในการพิจารณาคืนเงินให้แก่ผู้เสียหายกรณีที่บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลดังกล่าวได้รับการพิจารณาและพิสูจน์แล้วว่าไม่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี นอกจากนี้ กฎหมายยังกำหนดหน้าที่ให้สถาบันการเงิน ผู้ประกอบธุรกิจผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น ผู้ให้บริการอื่นที่เกี่ยวข้อง หรือผู้ให้บริการสื่อสังคมออนไลน์ “มีส่วนร่วมรับผิดชอบในความเสียหายที่เกิดจากอาชญากรรมทางเทคโนโลยี” เว้นแต่หน่วยงานหรือผู้ให้บริการข้างต้นจะพิสูจน์ได้ว่า ได้ปฏิบัติตามมาตรฐานหรือมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีตามที่กำหนดแล้ว[13] ในการนี้ **ธนาคารแห่งประเทศไทยจะออกประกาศเพื่อกำหนดมาตรฐานสำหรับสถาบันการเงิน (ธนาคารพาณิชย์และสถาบันการเงินเฉพาะกิจ) และผู้ประกอบธุรกิจบริการการชำระเงินที่ได้รับใบอนุญาตประเภทการให้บริการเงินอิเล็กทรอนิกส์ ซึ่งหากสถาบันการเงินและผู้ประกอบธุรกิจดังกล่าวละเลยการปฏิบัติตามมาตรฐานที่กำหนด จะต้องมีส่วนร่วมรับผิดชอบในความเสียหายแก่ลูกค้า** ตัวอย่างมาตราฐานที่จะถูกกำหนดในประกาศธนาคารแห่งประเทศไทยว่าด้วย “Shared Responsibility” อาทิ เพื่อการจำกัดความเสียหายและจัดการบัญชีม้า สถาบันการเงินต้องแจ้งเตือนการทำธุรกรรมทุกครั้งเมื่อมีการโอนเงินออกจากบัญชีผ่านช่องทางใดช่องทางหนึ่ง ไม่ว่าจะเป็น Mobile Banking, LINE, SMS, หรืออีเมล โดยไม่เรียกเก็บค่าใช้จ่าย ระงับการทำธุรกรรมและนำส่งข้อมูลตามแนวทางที่ศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) กำหนด และเมื่อได้รับรายชื่อบุคคลที่เป็นเจ้าของบัญชีม้าดำ (บัญชีของบุคคลที่เข้าข่ายการกระทำความผิดตามฐานข้อมูลสำนักงาน ปปง.) หรือรายชื่อบุคคลที่เป็นเจ้าของบัญชีม้าเทาเข้ม (บัญชีของบุคคลที่เกี่ยวข้องในเส้นทางการเงินทุจริตและถูกแจ้งความ) หรือบัญชีม้าเทา

[13] อริสรา กาญจนอุดม, **ยกระดับมาตรการรับมือภัยไซเบอร์ ด้วย พ.ร.ก. ว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568** [ออนไลน์], 20 มิถุนายน 2568. แหล่งที่มา: https://www.senate.go.th/view/386/News/Latest/320/TH-TH

อ่อน (บัญชีของบุคคลที่มีส่วนเกี่ยวข้องในเส้นทางการเงินทุจริต) จากระบบ Central Fraud Registry (CFR) ให้สถาบันการเงินดำเนินการให้สอดคล้องกับระดับความเสี่ยง เช่น ระงับเงินเข้าและออกทุกบัญชีของบุคคลที่เป็นเจ้าของบัญชีม้า รวมทั้งปฏิเสธการเปิดบัญชีใหม่ให้กับบุคคลที่เป็นเจ้าของบัญชีม้า เป็นต้น[14]

[14] ธนาคารแห่งประเทศไทย, **ธปท. กำหนดมาตรฐานของภาคธนาคารในการร่วมรับผิดชอบตาม พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี** [ออนไลน์], 20 มิถุนายน 2568. แหล่งที่มา: https://www.bot.or.th/th/news-and-media/news/news-20250428.html

รายการอ้างอิง

- กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี, **สถิติความเสียหายสะสม ตั้งแต่วันที่ 1 มกราคม 2568 ถึง วันที่ 3 กรกฎาคม 2568** [ออนไลน์], แหล่งที่มา: https://www.thaipoliceonline.go.th

- ธนาคารแห่งประเทศไทย, **ธปท. กำหนดมาตรฐานของภาคธนาคารในการร่วมรับผิดชอบตาม พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี** [ออนไลน์], แหล่งที่มา: https://www.bot.or.th/th/news-and-media/news/news-20250428.html

- ฝ่ายนวัตกรรมการเรียนรู้และสื่อสารองค์กร คณะนิติศาสตร์ มหาวิทยาลัยพะเยา, **ทำความรู้จัก พ.ร.ก. ป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และ (ร่าง) พรก. ไซเบอร์** [ออนไลน์], แหล่งที่มา: https://www.up.ac.th/NewsReadBlog2.aspx?itemID=33995

- พรเพ็ญ สดศรีชัย, **ว่าด้วยการ “ร่วมรับผิดชอบ” ความเสียหายจากภัยทางการเงิน** [ออนไลน์], แหล่งที่มา: https://www.bot.or.th/th/research-and-publications/articles-and-publications/articles/article-20250513.html

- มนูญธรรม ปรีชาไว, **ความรับผิดทางแพ่งจากการใช้บัตรเครดิต (กรณีมีเซลสลิป)**, วารสารกระบวนการยุติธรรม, ปีที่ 5 (พฤษภาคม-สิงหาคม 2555).

- ศีรวิษ สุขชัย และปริญญา ศรีเกตุ, **มาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี: ศึกษากรณีการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้า**, วารสารนวัตกรรมการศึกษาและการวิจัย, ปีที่ 8 ฉบับที่ 4 (ตุลาคม-ธันวาคม 2567).

- สภาองค์กรของผู้บริโภค, **ชนะคดี! ผู้บริโภคถูกแบงก์ฟ้อง โดนหลอกดูดเงินบัตรเครดิต** [ออนไลน์], แหล่งที่มา: https://www.tcc.or.th/17092567_consumer-sued_news/

- สภาองค์กรของผู้บริโภค, **ศาลเชียงใหม่ยกฟ้อง! กรณีไม่จ่ายหนี้บัตรเครดิตหลังผู้บริโภคโดนดูดเงิน** [ออนไลน์], แหล่งที่มา: https://www.tcc.or.th/dismiss-creditcard-fraud/

สภาองค์กรของผู้บริโภค, **ศาลยกฟ้อง กรณีถูกดูดเงินในบัตรกรุงไทยฯ** [ออนไลน์], แหล่งที่มา: https://www.tcc.or.th/dismiss-consumer-fraud/

อริสรา กาญจนอุดม, **ยกระดับมาตรการรับมือภัยไซเบอร์ ด้วย พ.ร.ก. ว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568** [ออนไลน์], แหล่งที่มา: https://www.senate.go.th/view/386/News/Latest/320/TH-TH