

## RESEARCH PAPER

# Rethinking the Legal Framework for Online Scams in Thailand: Lessons from the EU and US

### PANEL 1

### Deepfakes for Financial Fraud

## Dr. Saliltorn Thongmeensuk

---

Dr. Saliltorn Thongmeensuk is a Senior Research Fellow at the Thailand Development Research Institute (TDRI) and an Expert Fellow at Thailand's AI Governance Clinic (AIGC). She holds a Doctor of Laws (LL.D.) from Nagoya University, specializing in intellectual property. Dr. Thongmeensuk serves on the sub-committee drafting Thailand's Platform Economy Act and has led regulatory impact assessments on the Royal Decree on Digital Platforms. Her research focuses on platform liability, online scams, and AI governance. She is also an alumna of the U.S. IVLP on AI policy. She can be reached at [saliltorn@tdri.or.th](mailto:saliltorn@tdri.or.th).

## Nopphasin Camapaso

---

Nopphasin Camapaso is a Researcher at the Thailand Development Research Institute (TDRI), with a focus on digital policy, competition regulation, and the economic impacts of emerging technologies. His work explores issues such as artificial intelligence (AI), data governance, and labor market change. He has contributed to research related to platform regulation, copyright policy, and digital economy governance, supporting public sector initiatives and ongoing policy discussions. He can be reached at [nopphasin@tdri.or.th](mailto:nopphasin@tdri.or.th).

## Gavin Charoenkwan

---

Gavin Charoenkwan is a Research Assistant at the Thailand Development Research Institute and an incoming J.D. student at Harvard Law School. His main research interests include competition law and digital regulation, with a regional focus on Southeast Asia. Most recently, he was a contributing author to Europe in Review. He can be reached at [gavin.charoenkwan@gmail.com](mailto:gavin.charoenkwan@gmail.com).

*This paper is circulated for discussion and feedback. The views expressed are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, CfDS, Faculty of Social and Political Sciences UGM or any other organization. The author(s) welcome comments on this version and invite you to contact them directly with any feedback or questions.*



# Rethinking the Legal Framework for Online Scams in Thailand: Lessons from the EU and US

Dr. Saliltorn Thongmeensuk, Nopphasin Camapaso, Gavin Charoenkwan

The surge of online scams in Thailand has exposed critical weaknesses in the country's digital governance regime, prompting emergency legal reforms in 2023 and 2025. This paper argues that current Thai responses remain overly reactive, fragmented, and enforcement-centric, lacking the preventive legal architecture required to address structural risks embedded in digital platforms and financial systems. Drawing on comparative insights from the European Union and the United States, the paper identifies contrasting models: the EU's ex-ante, risk-based regulatory approach, exemplified by the Digital Services Act (DSA) and Payment Services Directives (PSD2/PSD3), and the U.S.'s post-incident enforcement and sectoral flexibility. Thailand's legal regime, by contrast, fails to impose cross-sectoral duties of care or incentivize platform accountability, while offering limited victim redress. This paper proposes a hybrid governance model that introduces risk-tiered platform obligations, statutory duties of care, real-time fraud intelligence sharing, and a centralized fraud oversight body. It concludes that effective digital fraud prevention requires legal frameworks that reconceptualize fraud as a systemic governance failure rather than isolated criminal acts, aligning liability with institutional capacity and technological influence.



## Introduction

The rapid evolution of digital services and financial technologies has created fertile ground for a rise in online scams, reshaping the global landscape of cybercrime and consumer vulnerability. Online fraud has become an increasingly pressing issue in Thailand, prompting significant concern among authorities and the public. In response, the Thai government has enacted emergency decrees in 2023<sup>1</sup> and 2025<sup>2</sup> aimed at enhancing measures for the prevention and suppression of technology crimes and regulating digital asset business operations. However, Thailand's legal infrastructure remains largely reactive, struggling to address the systemic risks embedded in the architecture of online platforms.

This article argues that Thailand must move beyond a fragmented enforcement approach and adopt a comprehensive legal framework that integrates platform responsibility, financial transaction security, and cross-sectoral coordination. Drawing on comparative insights from the European Union and the United States, it contends that online scams are not merely a matter of individual criminal conduct, but rather indicators of structural governance failures in the digital ecosystem. The EU's Digital Services Act (DSA) and Payment Services Directives (PSD2 and the forthcoming PSD3) provide a model of ex-ante, risk-based regulation, while the U.S. exemplifies a post-incident, enforcement-centric regime. Both approaches offer valuable lessons for recalibrating Thai law.

By analyzing current Thai legislation, enforcement practices, and regulatory gaps, this paper seeks to illuminate why existing measures fall short in preventing and remedying digital fraud. It further proposes legal and institutional reforms that would enable Thailand to build a more proactive, resilient, and victim-centered governance model for the digital age.

## The Landscape of Online Scams in Thailand

Online scams in Thailand have proliferated rapidly in both scale and sophistication, mirroring global trends while revealing distinct regional vulnerabilities. On average, more than 700 online fraud cases are reported daily in Thailand, with total damages exceeding 63 billion baht (USD 1.8 billion) between March 2022 and May 2024.<sup>3</sup> Scammers employ diverse tactics

---

<sup>1</sup> Emergency Decree on Measures for the Prevention and Suppression of Technology Crimes B.E. 2566 (2023).

<sup>2</sup> Emergency Decree on Digital Asset Businesses (No. 2) B.E. 2568 (2025).

<sup>3</sup> Royal Thai Police, Cyber Crime Investigation Bureau, Media Release, November 2023.

ranging from fraudulent advertisements to social engineering and identity theft via social media, text messages, or scam calls.<sup>4</sup>

Scam communications are increasingly AI-generated, making them more difficult to detect.<sup>5</sup> In February 2025, 163 victims were deceived by scammers using face-altering AI during video calls.<sup>6</sup> Similarly, the hacking group known as GoldFactory distributed a fake pension app that recorded victims' biometric videos to create deepfake content for unauthorized bank transfers.<sup>7</sup>

The economic impacts of these crimes are compounded by the erosion of public trust in digital platforms, posing long-term challenges for Thailand's digital economy and financial inclusion goals. A 2023 survey by the Electronic Transactions Development Agency (ETDA) found that 43% of Thai users were reluctant to engage in online transactions due to fraud concerns, with 29% reporting reduced mobile banking usage after exposure to scams.<sup>8</sup>

In response, the Thai government launched the Anti-Online Scam Operation Center (AOC 1441) in late 2023. The AOC has successfully frozen over 517,000 scammer-linked accounts and returned funds to victims in near real-time.<sup>9</sup> Similarly, the BoT has tightened biometric authentication requirements and mandated that commercial banks implement AI-driven fraud detection and facial recognition verification.<sup>10</sup> The Ministry of Digital Economy and Society (MDES) is preparing to launch the "DE-fence" platform by late 2025, using AI and big data analytics to monitor suspicious transactions and scam websites.<sup>11</sup>

Given that many fraud networks operate from outside Thailand, international cooperation is critical. In early 2025, Thailand and China announced the formation of joint cybercrime coordination centers in Bangkok and Mae Sot.<sup>12</sup> This led to the successful dismantling of a

---

<sup>4</sup> Ministry of Digital Economy and Society (MDES), "รวมว.คือ Kick off ศูนย์ AOC 1441 แก้ปัญหาหลอกลวงออนไลน์ แบบ One Stop Service สำหรับประชาชน" accessed February 28, 2025, <https://www.mdes.go.th/news/detail/7535>.

<sup>5</sup> Nation Thailand, "Govt sets up scam victim aid," December 26, 2024, <https://www.nationthailand.com/news/general/40042159>.

<sup>6</sup> Bangkok Post, "Two Men Arrested for Alleged B4M AI-Aided Scam Against Beauty Queen," January 15, 2025, <https://www.bangkokpost.com/thailand/general/2953450/two-men-arrested-for-alleged-b4m-ai-aided-scam-against-beauty-queen>.

<sup>7</sup> Group-IB, "GoldFactory iOS Trojan," accessed February 28, 2025, <https://www.group-ib.com/blog/goldfactory-ios-trojan/>.

<sup>8</sup> Electronic Transactions Development Agency (ETDA), 2023 Survey on Online Transaction Behavior.

<sup>9</sup> AM 549 KHz RadioThailand, "คือ ไซเบอร์ผลงานปราบโจรออนไลน์ 1 ปี เปิดศูนย์ AOC 1441 ระงับบัญชีต้องสงสัย 340,000 เคส - ความเสียหาย 1.9 หมื่นล้านบาท ปราบปรามจริงจังจนสถิติลดลง" (RadioThailand2025)

<https://edulampang.prd.go.th/th/content/category/detail/id/57/iid/340064>.

<sup>10</sup> Bank of Thailand (BoT), "Bank of Thailand Implements New Cybersecurity Measures," March 9, 2023, <https://www.bot.or.th/en/news-and-media/news/news-20230309.html>.

<sup>11</sup> DE-fence Platform. Accessed June 13, 2025. <https://www.thaigov.go.th/infographic/contents/details/8649>.

<sup>12</sup> Reuters, "Thailand, China Set Up Coordination Centre to Combat Scam Call Networks," January 24, 2025, <https://www.reuters.com/world/asia-pacific/thailand-china-set-up-coordination-centre-combat-scam-call-networks-2025-01-24>.



scam operation in Myawaddy, Myanmar, freeing over 7,000 trafficked individuals.<sup>13</sup> On a broader scale, Thailand also promoted regional collaboration through the ASEAN Working Group on Anti-Online Scam (WG-AS) and the ASEAN AI Governance Working Group (WG-AI), which now cooperate through a centralized cybersecurity coordination center.<sup>13</sup>

## Legal and Regulatory Framework in Thailand

Thailand's evolving legal framework against online fraud reflects a state-led enforcement model that remains largely reactive. The country continues to rely on criminal statutes and incident-driven regulatory tools. The system is fragmented, with overlapping jurisdiction among digital, financial, and telecommunications regulators.

### Platform Regulation under the Royal Decree B.E. 2565 (2022) (The Royal Decree)

The Royal Decree on Digital Platform Services B.E. 2565, enforced by the ETDA, represents the country's first comprehensive attempt to regulate digital platforms operating within its jurisdiction, including foreign entities that provide services to users in Thailand. Its primary thrust is procedural: requiring platforms to register with ETDA,<sup>14</sup> appoint a local representative if based overseas,<sup>15</sup> and submit compliance reports.<sup>16</sup>

The Decree applies universally to covered digital services, but it introduces an additional layer of regulatory obligations for a subset designated as "specified platforms."<sup>17</sup> This designation, based on criteria such as platform size, user base, and potential impact, triggers enhanced requirements, including internal complaint mechanisms, stricter transparency obligations, and more extensive cooperation with regulatory authorities. While this risk-tiered distinction echoes certain features of the EU's DSA, the Royal Decree does not adopt the its system of ex-ante obligations like risk assessments<sup>18</sup> or content moderation policies.<sup>19</sup>

<sup>13</sup> ASEAN, "Bangkok Digital Declaration," January 2025, <https://asean.org/wp-content/uploads/2025/01/14-ENDORSED-BANGKOK-DIGITAL-DECLARATION.pdf>.

<sup>14</sup> Royal Decree on Digital Platform Services B.E. 2565 (2022), s 8.

<sup>15</sup> *ibid*, s 11.

<sup>16</sup> *ibid*, s 22.

<sup>17</sup> *ibid*, s 18.

<sup>18</sup> The Royal Decree contains no provision requiring **systemic risk assessments** for platforms, even those designated as "specified platforms." This contrasts with the DSA's Article 34, which mandates Very Large Online Platforms (VLOPs) to conduct and update risk assessments covering illegal content, fundamental rights, and civic discourse.

<sup>19</sup> While the Royal Decree on Digital Platform Services B.E. 2565 imposes a limited obligation for specified platforms to disclose the main parameters of their recommendation systems in Section 17, it does not establish broader algorithmic accountability or risk mitigation duties as found in the EU Digital Services Act. The Thai

Crucially, the Thai framework does not impose proactive duties of care on platforms regarding scam mitigation or fraud prevention. This contrasts sharply with the DSA, which explicitly mandates that Very Large Online Platforms (VLOPs) must identify and mitigate systemic risks, including risks related to illegal content and disinformation.<sup>20</sup>

## **Enforcement under the Emergency Decree on the Prevention and Suppression of Technology Crime B.E. 2566 (2023)**

---

The Emergency Decree on the Prevention and Suppression of Technology Crime B.E. 2566 (2023) expanded the investigative powers of state agencies, including the Royal Thai Police, Anti-Money Laundering Office (AMLO), and Department of Special Investigation (DSI).<sup>21</sup> The law authorizes these agencies to freeze suspicious accounts, block content deemed illegal, and coordinate cross-border information requests.<sup>22</sup> However, the decree centers almost entirely on post-incident enforcement, rather than the systemic risk management approach found in jurisdictions like the EU. There is no requirement for operators to assess scam risks, disclose systemic vulnerabilities, or implement predictive detection systems. Victim protection mechanisms, such as restitution or fund recovery, are often slow, and many digital crimes remain unresolved due to jurisdictional fragmentation or insufficient evidence.

## **Two Draft Emergency Decrees for Technology Crime and Digital Assets**

---

On April 8, 2025, the Thai Cabinet approved two new emergency decrees:

1. Draft Emergency Decree on Measures for the Prevention and Suppression of Technology Crime (No. 2) B.E. 2568
2. Draft Emergency Decree on Digital Asset Business Operations (No. 2) B.E. 2568

The first decree significantly expands state powers and introduces horizontal obligations across the private sector:

- Expanded the scope of “digital business operators” to include wallet services, e-money accounts, and offshore service providers targeting Thai users.

---

approach reflects a transparency-lite model, lacking user control options or systemic auditability of algorithmic harms.

<sup>20</sup> Digital Services Act (2022), art 35.

<sup>21</sup> Emergency Decree on the Prevention and Suppression of Technology Crime B.E. 2566 (2023), s 4.

<sup>22</sup> *ibid*, s 4–6.

- Mandated content filtering for messages that “clearly appear” to solicit fraud even before a user clicks into them.
- Implemented a private-sector proof-of-compliance obligation, requiring businesses to demonstrate they followed state-mandated fraud prevention standards to avoid liability.
- Increased corporate and individual penalties, including imprisonment for directors of negligent service providers.
- Enacted data-sharing mandates between SEC, NBTC, and enforcement agencies to trace suspicious digital asset movements.

The second decree extends extraterritorial reach by requiring non-Thai digital asset businesses to register and comply if they serve users in Thailand.<sup>23</sup>

Thailand’s new decrees primarily rely on enhanced state surveillance powers and cross-agency enforcement mandates. However, the imposition of screening duties on telecommunications and digital asset providers risks overburdening private actors without ensuring procedural safeguards. Furthermore, the decrees adopt a largely punitive posture, including the threat of criminal sanctions for corporate directors, rather than incentivizing systemic fraud-prevention. In addition, it remains unclear whether Thai regulators possess the leverage to compel foreign actors to register and comply, particularly in the absence of mutual legal assistance treaties.

## Comparative Insights: The EU and US

The global escalation of online fraud and scam has compelled governments to move toward more anticipatory regulatory responses. In this shift, the European Union and the United States represent divergent models. The EU’s approach is typified by ex-ante, rights-based, and platform-oriented governance, whereas the US emphasizes ex-post enforcement, operational intelligence, and prosecutorial flexibility.

### Platform Responsibility vs. Enforcement-Centered Strategy

The European Union’s ex-ante model is codified most notably in the DSA. This regulation imposes legal obligations most critically on platforms classified as VLOPs and Very Large

---

<sup>23</sup> Draft Emergency Decree on Digital Asset Business Operations (No. 2) B.E. 2568, s 4.



Online Search Engines (VLOSEs) which reach more than 45 million users per month within the EU.<sup>24</sup> DSA Article 34 requires that VLOPs conduct annual systemic risk assessments focusing on illegal content, fundamental rights violations, and manipulation of platform services.<sup>25</sup> Upon identifying risks, platforms must implement proportionate mitigation measures.<sup>26</sup> Article 37 requires that VLOPs undergo independent audits.<sup>27</sup> The legal principle underlying the DSA is platform due diligence, analogous to fiduciary duties in financial regulation, wherein platforms must foresee and prevent foreseeable harm arising from their systemic function.

In contrast, the United States' model remains rooted in ex-post enforcement, drawing upon sector-specific statutes and prosecutorial discretion. Regulatory responsibility is dispersed across federal agencies such as the Federal Trade Commission (FTC) and the Federal Bureau of Investigation (FBI). The FTC uses its authority under Section 5 of the FTC Act to pursue unfair or deceptive trade practices, while the FBI coordinates cybercrime investigations through the Internet Crime Complaint Center (IC3).

Compounding this reactive model is Section 230 of the Communications Decency Act (47 U.S.C. § 230), which immunizes platforms from liability for third-party content, except under narrow circumstances (e.g., when platforms materially contribute to illegality).<sup>5</sup> Efforts to reform this legal shield have emerged in Congress (e.g., the SAFE TECH Act,<sup>28</sup> PATA Act<sup>29</sup>), but none have succeeded in shifting the legal burden onto platforms to prevent fraud ex-ante.

Unlike the EU's DSA, the U.S. model lacks legally mandated risk assessments, ad transparency, or systemic audit mechanisms. Instead, the FTC may bring enforcement cases when a company's practices violate consumer protection standards.<sup>30</sup> This may result in platforms adopting minimal compliance postures, and fraud may proliferate within opaque ad networks and recommendation engines.

For countries like Thailand, the comparative lesson is that fraud in the digital economy cannot be fully addressed through enforcement alone. It requires infrastructure-level intervention,

---

<sup>24</sup> Digital Services Act (2022), arts. 33–43.

<sup>25</sup> *ibid*, art 34.

<sup>26</sup> *ibid*, art 35.

<sup>27</sup> *ibid*, art 37.

<sup>28</sup> **SAFE TECH Act:** Introduced by Senators Mark Warner, Mazie Hirono, and Amy Klobuchar, the Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms (SAFE TECH) Act seeks to narrow the scope of Section 230 immunity.

<sup>29</sup> **PACT Act:** The Platform Accountability and Consumer Transparency (PACT) Act, introduced by Senators Brian Schatz and John Thune, aims to increase transparency and accountability of online platforms.

<sup>30</sup> Federal Trade Commission Act 15 USC § 45 (2018).

particularly for fraud that arises from platform architecture. The EU's DSA therefore offers a more sustainable model for Thailand's regulatory future.

## Europe's Legal Toolkit

---

The EU's framework combines platform governance (DSA) with financial transaction security (PSD2/PSD3). The Payment Services Directive 2 (PSD2), in force since 2018, mandates Strong Customer Authentication (SCA) for online payments, requiring two or more factors for transactions.<sup>31</sup> Evidence shows that Europe saw a 47 percent reduction in fraud pressure since the SCA became mandatory<sup>32</sup>. However, the introduction of stricter authentication methods might stall redirections from the merchant site to the bank, prolonging transactions. Consequently, the early introduction of 3D secure transactions saw a 30 percent abandon rate by the customer.<sup>33</sup>

Furthermore, while PSD2 successfully reduced fraud at the payment authorization stage, it did little to prevent social engineering scams, particularly those that rely on impersonation, manipulated trust, or fraudulent advertisements. In these cases, the transaction itself may be technically secure, but the user intent has been manipulated through upstream deceptive design.

Recognizing a need for more extensive measures, the European Commission proposed the PSD3 and the Payment Services Regulation (PSR) in June 2023. Notably, Article 59 of the draft PSR introduces conditional liability for digital platforms, particularly when fraud arises from advertising or communication features that platforms control.<sup>34</sup> This transforms platform liability from a question of direct causation (did the platform itself defraud the user?) to a question of risk capacity (could the platform have prevented this harm?). This new duty reflects what scholars increasingly describe as horizontal risk governance, where the duty to prevent harm is distributed not only to the primary actor (e.g., the scammer) but across a network of technologically capable intermediaries based on their capacity to address systemic harm, even in the absence of direct culpability. This theory mirrors evolving

---

<sup>31</sup> Payment Services Directive 2 (2015), art 97.

<sup>32</sup> Cassidy, Mike. "3D Secure Authentication: The Good, the Bad and What It Means for Your Fraud Prevention." Signifyd, July 2, 2024. <https://www.signifyd.com/blog/3d-secure-authentication-the-good-the-bad-and-what-it-means-for-your-fraud-prevention/>.

<sup>33</sup> Rolfe, Alex. "Worldwide Trends in Increasing Payment Regulation and 3D Secure 2.0." Payments Cards & Mobile, October 11, 2019. <https://www.paymentscardsandmobile.com/worldwide-trends-in-increasing-payment-regulation-and-3d-secure-2-0/>.

<sup>34</sup> Payment Services Regulation (PSR), art. 59.

obligations in other domains such as environmental law (e.g., supply chain responsibility) and cybersecurity (e.g., critical infrastructure risk management).

Furthermore, the PSR proposal also introduces several other fraud-reduction measures, such as:

- Enhanced transparency obligations for banks and payment providers regarding refund eligibility and reasons for refusal;
- Mandatory fraud awareness education campaigns to be coordinated at the EU level;
- Real-time transaction monitoring systems to detect unusual payment behavior;
- Improved dispute resolution mechanisms and faster refund rights for victims of authorized push payment (APP) fraud.<sup>35</sup>

For legal scholars, PSD3 illustrates how fragmented regulatory silos can be re-integrated to address cross-system risks like fraud. It also shows how liability rules are evolving from models of strict fault-based enforcement to models that emphasize institutional duty of care, particularly when actors occupy gatekeeping positions in networked ecosystems. This evolution signifies a legal recognition that in the age of algorithmic content delivery, paid amplification, and cross-border real-time payments, fraud is a systemic externality and must be governed as such.

## Contesting the Boundaries of Legal Duty


---

The global struggle to combat online fraud has exposed the fragility of legal boundaries. As regulators attempt to reassign responsibility for harm, they inevitably encounter resistance from entrenched institutions. Nowhere is this more visible than in the debates surrounding Article 59 of the PSR and the ongoing U.S. efforts to reform Section 230 of the Communications Decency Act.

In the European Union, Article 59 of PSR represents a bold conceptual leap. It proposes conditional liability for digital platforms where consumer fraud arises from features they control or monetize, such as paid advertisements or messaging systems. This introduces a risk-based duty, shifting the burden of mitigation onto those best positioned to prevent deception, even where their conduct is not directly illegal or negligent.

---

<sup>35</sup> *ibid.*



Unsurprisingly, this move has provoked substantial industry pushback. CCIA Europe, representing major technology firms, has argued that Article 59 creates vague and potentially unbounded liability, inconsistent with the DSA's tiered "due diligence" framework. According to this critique, PSD3 risks creating a chilling effect on platform innovation and user-generated content ecosystems by over-censoring or withdrawing critical features—such as open messaging, real-time ad tools, or small advertiser onboarding—out of fear of liability for user misuse.

This critique reveals a deeper fault line: the tension between ex-ante systemic regulation (as seen in the DSA) and ex-post transactional liability (as introduced in PSD3). While both instruments are part of the EU's broader digital governance architecture, they are rooted in different regulatory traditions. This expansion risks undermining legal coherence. If platforms are held liable under PSD3 for failure to prevent fraud linked to advertising but retain immunity for similar failures under the DSA (due to good faith content moderation), the result could be regulatory fragmentation and legal uncertainty.

The United States, meanwhile, grapples with a different yet related tension: the durability of Section 230 of the Communications Decency Act (47 U.S.C. § 230). Enacted in 1996, Section 230 provides broad immunity to online intermediaries for content posted by third parties, with limited exceptions for intellectual property, federal criminal law, sex trafficking, and electronic privacy violation.<sup>36</sup> While historically credited with enabling the rise of the modern internet, critics now argue that this immunity inhibits accountability, especially when platforms amplify, monetize, or algorithmically rank fraudulent content.<sup>37</sup>

In recent years, multiple reform proposals have sought to narrow this immunity. The SAFE TECH Act, introduced in the Senate, would remove Section 230 protections for content involving "paid advertisements" or harmful conduct, including civil rights violations and targeted harassment.<sup>38</sup> Similarly, the Protecting Americans from Dangerous Algorithms Act would eliminate Section 230 immunity where platforms use algorithms to recommend content that leads to physical or financial harm.<sup>39</sup>

However, these reform efforts have met with strong resistance. Critics argue that narrowing Section 230 could have a chilling effect on free expression, as platforms might preemptively

---

<sup>36</sup> Communications Decency Act, 47 USC § 230 (2018)

<sup>37</sup> Kate Ruane, 'Dear Congress: Platform Accountability Should Not Threaten Online Expression' (*American Civil Liberties Union* 27 October 2020)

<sup>38</sup> SAFE TECH Act, S.560, 118th Cong (2023)

<sup>39</sup> Protecting Americans from Dangerous Algorithms Act, H.R. 2154, 117th Cong (2021)

restrict user speech to avoid legal exposure.<sup>40</sup> There is also concern that liability carve-outs would disproportionately harm smaller platforms, which lack the legal and technical capacity to vet every piece of content or advertisement.<sup>41</sup> Furthermore, opponents warn that such reforms could blur the line between publisher and platform, undermining the legal scaffolding that has enabled diverse forms of digital interaction, from user forums to independent journalism.<sup>42</sup>

Across both jurisdictions, we therefore witness a governance paradox. While regulators recognize that algorithms have systemic and manipulative power, legal doctrine and institutional inertia resist holding platforms legally responsible for harms they did not directly cause. This paradox is intensified by the economic model of platforms, which incentivizes engagement at scale, often regardless of content accuracy or risk. Attempts to reassign duty run up against the architecture of digital capitalism, which rewards virality, personalization, and monetization, even where these mechanisms facilitate fraud.<sup>43</sup> Neither jurisdiction has arrived at a fully coherent model. The EU's layered system may offer greater protection but risks overburdening platforms with diffuse obligations, while the U.S. model preserves flexibility but permits systemic under-regulation, especially in the realm of fraud.

For regulators abroad, this juncture offers a cautionary tale. The question is not only how much liability to impose, but also how to align that liability with institutional capacity, constitutional norms, and market structure. A governance framework that misallocates duty may either entrench impunity or stifle innovation. The challenge is to design legal obligations that reflect platform influence without collapsing under enforcement ambiguity or political resistance.

## Legal and Governance Gaps in Thailand

Despite Thailand's increasing legislative activity in response to the rise of online scams, its legal and governance framework remains reactive, fragmented, and insufficiently aligned with global best practices. While Thai authorities have taken steps to modernize enforcement

---

<sup>40</sup> Alan Rozenshtein, 'Interpreting the Ambiguities of Section 230 - Yale Journal on Regulation' (2024) Yale Journal on Regulation

<sup>41</sup> Cameron F Kerry, 'Section 230 Reform Deserves Careful and Focused Consideration' (*Brookings Institution* 14 May 2021).

<sup>42</sup> *ibid.*

<sup>43</sup> Jiadong Yu, DA Bekerian and Chelsea Osback, 'Navigating the Digital Landscape: Challenges and Barriers to Effective Information Use on the Internet' (2024) 4 *Encyclopedia* 1665.

capacity, the current approach remains centered on post-incident remedies, without imposing preventative obligations on platforms or intermediaries.

The Royal Decree on Digital Platform Services, administered by the ETDA, requires that certain digital service providers register, appoint a local representative, and provide basic compliance documentation.<sup>44</sup> However, the decree does not mandate that platforms implement ex ante measures to prevent fraud. In this regard, Thailand diverges sharply from the DSA, which imposes legally binding duties on VLOPs to assess systemic risks, including those related to fraudulent advertising, and to adopt proportionate mitigation strategies under Articles 34 and 35.<sup>45</sup>

The emphasis in Thailand remains largely enforcement-centric. The Emergency Decree on Cybercrime B.E. 2566 enables police and administrative authorities to freeze accounts, block telecommunications services, and remove illegal digital content.<sup>46</sup> Yet, these measures are difficult to coordinate in practice. Inter-agency fragmentation persists, with overlapping mandates among the Royal Thai Police, AMLO, and the Ministry of Digital Economy and Society leading to delays and inconsistent responses to fraud complaints,

Moreover, Thailand's legal regime continues to struggle with non-criminal but deceptive practices, such as fake online reviews, influencer-led investment promotions, and emotional manipulation in romance scams. They are neither easily classified as criminal offenses under existing penal statutes, nor clearly within the scope of civil or administrative sanction. The Office of the Consumer Protection Board (OCPB), for instance, has limited jurisdiction over fraudulent advertisements that emerge through peer-to-peer platforms or influencer channels, particularly when the promotional content does not meet the formal legal definition of advertising under Thai law<sup>47</sup>.

In April 2025, the Thai Cabinet approved two new emergency decrees in response to escalating public concern: the Emergency Decree on Measures for the Prevention and Suppression of Technology Crime (2024) and the Emergency Decree on Digital Asset Business Operations (2024), which represent an expansion of the regulatory perimeter. Among the most notable innovations are new duties imposed on platforms to identify and suppress messages that clearly appear fraudulent without requiring the user to interact with the content.<sup>48</sup> Platforms must also support inter-agency data sharing about digital wallets

---

<sup>44</sup> Royal Decree on Digital Platform Services B.E. 2565, ss. 11, 18, 22.

<sup>45</sup> DSA, arts. 34–35.

<sup>46</sup> Emergency Decree on the Prevention and Suppression of Technology Crime B.E. 2566 (2023), ss. 4–6.

<sup>47</sup> Thailand Research and Development Institute, Regulatory Assessment on Digital Platform Act, 2024

<sup>48</sup> Emergency Decree on Measures for the Prevention and Suppression of Technology Crime (2025), s 6.



linked to illicit activities.<sup>49</sup> Furthermore, digital businesses are now subject to a burden of proof standard: they must show compliance with government-prescribed anti-fraud standards in order to escape liability.<sup>50</sup>

The new decrees further extend legal liability to include digital asset service providers operating outside Thailand's borders but targeting Thai consumers. Criteria such as offering services in Thai language, accepting baht payments, or choosing Thai law as governing law trigger jurisdiction.<sup>51</sup> Moreover, liability has been expanded to include criminal penalties for directors and officers intentionally participate in fraudulent activities.<sup>52</sup> These reforms are significant, but still rely heavily on enforcement after the fact and stop short of embedding obligations akin to risk-based audits, algorithmic transparency, or notice-and-action regimes found in the DSA.

What remains absent is a coordinated fraud governance ecosystem that allows for preventive intervention, cross-sector information sharing, and measurable accountability benchmarks. Unlike the European Union, which assigns ex ante duties to platforms based on size and influence, Thailand imposes one-size-fits-all reporting obligations without calibrating regulatory expectations to risk exposure. And unlike the United States, where the IC3 serves as a national coordination hub, Thailand lacks a centralized mechanism for addressing fraud reports. The April 2024 decree does create a Technology Crime Suppression Center under the Ministry of Digital Economy and Society, but its mandate, operational independence, and integration with law enforcement remain undefined as of this writing.<sup>53</sup>

Further, victims' access to redress remains underdeveloped. While the new decree includes a framework for refunding victims, including forfeiture mechanisms for unclaimed assets and timelines for victim claims, the success of these provisions will depend on detailed sub-regulations yet to be issued. Civil liability also remains ambiguous. Current Thai tort law does not clearly impose duties on platforms to protect users from fraud committed by third parties, and contractual remedies are difficult to pursue given the complexity of transnational digital platforms.

In summary, Thailand's legal architecture is characterized by strong enforcement rhetoric but weak systemic prevention. The April 2024 decrees mark a meaningful evolution, particularly

---


<sup>49</sup> *ibid*, s 4.

<sup>50</sup> The Standard Team, 'กรม. เห็นชอบ 2 ร่าง พ.ร.บ.ไซเบอร์ "คุมเงินดิจิทัล-สกัดอาชญากรรม"' (The Standard 8 April 2025) <https://thestandard.co/cabinet-cyber-decree-drafts/>.

<sup>51</sup> Emergency Decree on Digital Asset Business Operations (2025), s 4.

<sup>52</sup> Emergency Decree on Measures for the Prevention and Suppression of Technology Crime (2025), s 10.

<sup>53</sup> *ibid*, s 13.



in relation to digital asset regulation, but they remain bound to a paradigm of post hoc enforcement. To align with international best practices, Thailand must embed a governance framework that combines ex ante platform obligations, risk-tiered oversight, and cross-sector cooperation.

## Policy Recommendations


To align with emerging global best practices, Thailand must pursue a reconceptualization of fraud governance. First, it should codify tiered platform obligations based on user base size, economic impact, and risk exposure, akin to the DSA's designation of VLOPs. This would ensure that dominant platforms are held to higher transparency and prevention standards, particularly in relation to monetized features like advertising and messaging that are routinely exploited for scams.

Second, Thailand should mandate real-time data sharing and incident coordination between banks, digital platforms, and enforcement agencies. While the Emergency Decree on Cybercrime allows for information requests and service suspensions, it does not establish structured protocols for proactive collaboration. A dedicated statutory framework for cross-sectoral threat intelligence sharing—with safeguards for data privacy—would significantly enhance response speed and fraud containment.

Third, there is a need for a centralized fraud governance agency, modeled perhaps on the EU's national Digital Services Coordinators or the U.S. IC3. Such a unit could serve as the nucleus for incident response, regulatory oversight, user complaint redress, and strategic policy formulation. Its mandate should include producing public transparency reports, facilitating whistleblower channels, and coordinating with international cybercrime networks.

Fourth, Thailand should legislate civil liability pathways for victims of non-criminal scams, particularly those involving deception via advertisements, fake reviews, and influencer promotions. These harms, while often excluded from the criminal justice system, cause measurable financial and psychological damage and should be actionable under consumer protection or digital tort law, consistent with global trends in digital accountability.

Fifth, Thailand must introduce statutory duties of care for platforms, particularly in relation to high-risk functions such as messaging features, wallet integrations, payment links, and algorithmic amplification. Such duties would not require platforms to guarantee the absence of fraud, but rather to adopt industry-standard preventive practices and demonstrate their



implementation when harm occurs to incentivize investment in trust and safety infrastructures and discourage the externalization of risk to users.

More broadly, Thailand must move beyond the notion of fraud as a series of isolated incidents and instead recognize it as an infrastructural failure of digital governance. The technical affordances of digital platforms render fraud not merely a criminal aberration but a predictable systemic risk. Legislation must therefore be recalibrated to govern the architecture of interaction itself, embedding resilience at the level of code, algorithm, and interface design.

Ultimately, Thailand's future in online fraud prevention will depend not only on stronger criminal enforcement but also on its willingness to legislate responsibility across the full spectrum of digital stakeholders. The EU's model of ex ante duties and horizontal coordination, and the U.S.'s investigative agility and civil enforcement, each offer lessons. But Thailand must build a hybrid model suited to its institutional capacities, socio-economic realities, and platform ecology. Only then can it transition from reactive crisis management to a mature system of preventive digital governance, capable of safeguarding its citizens in an increasingly deceptive online world.

## Bibliography

AM 549 KHz RadioThailand, 'ดีอี โชว์ผลงานปราบโจรออนไลน์ 1 ปี เปิดศูนย์ AOC 1441 ระงับบัญชีต้องสงสัย 340,000

เคส - ความเสียหาย 1.9 หมื่นล้านบาท ปราบปรามจริงจังจนสถิติลดลง' (RadioThailand2025)

<<https://edulampang.prd.go.th/th/content/category/detail/id/57/iid/340064>>

ASEAN, 'Bangkok Digital Declaration' (ASEAN2025) <[https://asean.org/wp-](https://asean.org/wp-content/uploads/2025/01/14-ENDORSED-BANGKOK-DIGITAL-DECLARATION.pdf)

[content/uploads/2025/01/14-ENDORSED-BANGKOK-DIGITAL-DECLARATION.pdf](https://asean.org/wp-content/uploads/2025/01/14-ENDORSED-BANGKOK-DIGITAL-DECLARATION.pdf)>

Bank of Thailand, 'The Bank of Thailand Issues Additional Measures to Combat Financial

Fraudulent Activities.' (Bank of Thailand2023) <[https://www.bot.or.th/en/news-and-](https://www.bot.or.th/en/news-and-media/news/news-20230309.html)

[media/news/news-20230309.html](https://www.bot.or.th/en/news-and-media/news/news-20230309.html)>

Cassidy M, '3D Secure Authentication: The Good, the Bad and What It Means for Your Fraud

Prevention' (Signifyd24 April 2024) <[https://www.signifyd.com/blog/3d-secure-](https://www.signifyd.com/blog/3d-secure-authentication-the-good-the-bad-and-what-it-means-for-your-fraud-prevention)

[authentication-the-good-the-bad-and-what-it-means-for-your-fraud-prevention](https://www.signifyd.com/blog/3d-secure-authentication-the-good-the-bad-and-what-it-means-for-your-fraud-prevention)>

Electronic Transactions Development Agency, '2023 Survey on Online Transaction Behavior'

(2023)

Kerry C, 'Section 230 Reform Deserves Careful and Focused Consideration' (Brookings

Institution14 May 2021) <[https://www.brookings.edu/articles/section-230-reform-](https://www.brookings.edu/articles/section-230-reform-deserves-careful-and-focused-consideration/)

[deserves-careful-and-focused-consideration/](https://www.brookings.edu/articles/section-230-reform-deserves-careful-and-focused-consideration/)>

Ministry of Digital Economy and Society, 'รวมดีอี Kick off ศูนย์ AOC 1441 แก้ปัญหาหลอกลวงออนไลน์ แบบ

One Stop Service สำหรับประชาชน' (2023) <<https://www.mdes.go.th/news/detail/7535>>

Nation Thailand, 'Over a Quarter of Thais Targeted by Scams over Past Year' (Nation

Thailand8 October 2024)

<<https://www.nationthailand.com/news/general/40042159>>

Panarat Thepgumpanat and Panu Wongcha-um, 'Thailand and China to Set up Coordination Centre to Combat Scam Call Networks' Reuters (24 January 2025)

<<https://www.reuters.com/world/asia-pacific/thailand-china-set-up-coordination-centre-combat-scam-call-networks-2025-01-24/>>

Polovinkin A and Low S, 'GoldFactory IOS Trojan' (Group-IB2024) <[https://www.group-](https://www.group-ib.com/blog/goldfactory-ios-trojan/)

[ib.com/blog/goldfactory-ios-trojan/](https://www.group-ib.com/blog/goldfactory-ios-trojan/)>

Rolfe A, 'Worldwide Trends in Increasing Payment Regulation and 3D Secure 2.0' (Payments

Cards & Mobile11 October 2019)

<<https://www.paymentscardsandmobile.com/worldwide-trends-in-increasing-payment-regulation-and-3d-secure-2-0/>>

Royal Thai Government, 'DE-Fence Platform' (Royal Thai Government 2025)

<<https://www.thaigov.go.th/infographic/contents/details/8649>>

Royal Thai Police, Cyber Crime Investigation Bureau, 'Media Release, November 2023' (2023)

Rozenshtein A, 'Interpreting the Ambiguities of Section 230' [2024] Yale Journal on Regulation <<https://www.yalejreg.com/bulletin/interpreting-the-ambiguities-of-section-230/>>

Thailand Research and Development Institute, 'Regulatory Assessment on Digital Platform Act' (2024)

The Standard Team, 'กรม. เห็นชอบ 2 ร่าง พ.ร.บ. ไซเบอร์ "คุมเงินดิจิทัล-สกัดอาชญากรรม"' (The Standard 8 April 2025)

<<https://thestandard.co/cabinet-cyber-decree-drafts/>>

Wassayos Ngamkham, 'Two Men Arrested for Alleged B4m AI-Aided Scam against Beauty Queen' (<https://www.bangkokpost.com> 3 February 2025)

<<https://www.bangkokpost.com/thailand/general/2953450/two-men-arrested-for-alleged-b4m-ai-aided-scam-against-beauty-queen>>

Yu J, Bekerian DA and Osback C, 'Navigating the Digital Landscape: Challenges and Barriers to Effective Information Use on the Internet' (2024) 4 Encyclopedia 1665

Communications Decency Act, 47 USC § 230 2018

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC 2015

Emergency Decree on Digital Asset Business Operations (No. 2) B.E. 2568 2025

Emergency Decree on Measures for the Prevention and Suppression of Technology Crimes B.E. 2566 2023

Federal Trade Commission Act, 15 U.S.C. § 45 2018



Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on  
Payment Services in the Internal Market and Amending Regulation (EU) No 1093/2010  
2023

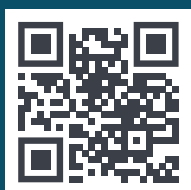
Protecting Americans from Dangerous Algorithms Act, H.R. 2154, 117th Cong 2021

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October  
2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC  
(Digital Services Act) 2022

Royal Decree on Digital Platform Services B.E. 2565 2022

SAFE TECH Act, S.560, 118th Cong 2023





INFORMATION RESILIENCE & INTEGRITY SYMPOSIUM

Generative AI and Information Resilience  
in the Asia-Pacific: Actions and Adaptations

➤ Faculty of Social and Political Sciences  
Universitas Gadjah Mada

➤ 21 August 2025