STIMSON

EXPLAINER

Trade & Technology

Cyber & Southeast Asia Programs

Countering Cyber Scam Operations Project

July 2025

# Countering Digital Deception: National Responses to Online Scams

**As cyber scam compounds proliferate, target countries are stepping up responses to safeguard national security and economic stability**

By **Allison Pytlak** Co-Author • **Brian Eyler** Co-Author • **Courtney Weatherby** Co-Author • **Kathleen Scoggin** Research • **Shreya Lad** Research

**Cyber scams have rapidly emerged as a critical security concern over the past two years, with INTERPOL labeling the threat as a "global crisis." These organized operations span multiple countries but are especially concentrated in special economic zones (SEZs) and fragile areas in the Indo-Pacific, particularly in Southeast Asia, where transnational criminal groups exploit weak governance, rapid digitalization, cryptocurrency markets, and limited law enforcement capacity. Th expansion of cyber-enabled fraud is driving staggering global financial losses, undermining national security and economic prosperity, and fueling trafficking in persons to staff scam compounds. These crimes ripple outward, straining rule of law in host countries and burdening economies of target countries.**

**This explainer provides an overview of how scam centers operate, outlines common types of online fraud, and profiles national responses from key target countries, including the United States, Canada, and Australia and across Southeast Asia.**

This resource is part of the broader Countering Cyber Scam Operations Project implemented jointly by the Cyber and Southeast Asia Programs at the Stimson Center, with support from Global Affairs Canada.

Thank you to those who took the time to review these profiles:

**Toby Evans**, Head of Economic Crime, Auspaynet

**Jeff Thomson**, Acting Manager In Charge, Canadian Anti-Fraud Centre, Royal Canadian Mounted Police

**Allan Cabanlong,** Southeast Asia Hub Director, Global Forum on Cyber Expertise (GFCE)

**Helena Yixin Huang**, Associate Research Fellow, Executive Deputy Chairman's Office at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore

**Andrew Wasuwongse**, Director, International Justice Mission Thailand

**Kathryn Westmore**, Senior Research Fellow, Centre for Finance and Security, the Royal United Services Institute

**Erin West**, Founder, Operation Shamrock

## Contents

## Introduction

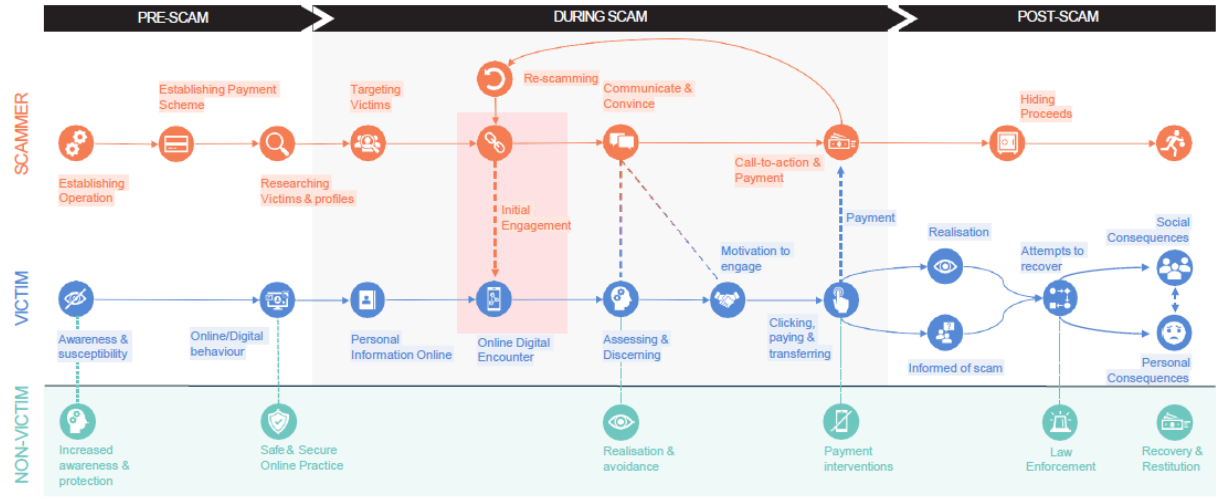
Cyber-enabled fraud, or "cyber scams," have emerged as an increasingly urgent security concern in the last two years. The compounds out of which they operate exist in multiple locations globally but have been most prolific in the special economic zones (SEZs) and fragile spaces in the Indo-Pacific region, especially Southeast Asia, where they have rapidly altered the transnational organized crime landscape. Technological developments, combined with rapid digitalization, weak governance, limited law enforcement capability in the areas where scam centers are most concentrated, and lax regulation of key markets like cryptocurrency have created a perfect storm for criminal enterprises to rapidly and efficiently scale-up their operations. This is leading to significant financial losses worldwide, often with a heavy emotional toll for scam victims. Scam centers rely on forced labor, trafficking in persons, or lack of economic opportunity to 'staff' their operations, in which many people work in support or peripheral roles unrelated to direct scamming activity. Cyber-enabled fraud and scams challenge the rule of law and human rights in their host countries, while causing ripple effects and economic burdens for primary victim economies and increasingly threatening national, regional, and global security. In 2023, the International Criminal Police Organization (INTERPOL) labelled it as a "global crisis representing a serious and imminent threat to public safety."[1]

### WHAT ARE SOME COMMON TYPES OF ONLINE SCAMS AND FRAUD?

An online scam occurs when someone is tricked into giving away personal information, financial details, or money via the Internet. Email scams have been around since the start of the online era, but modern scams make greater use of messaging services, social media, false websites, and even personal information databases obtained illicitly through the dark web or data breaches. Criminal networks also use fake job advertisements or immigration offers to lure individuals into 'working' for the scam centers and compounds.[2] The mainstream proliferation of generative artificial intelligence (GenAI) allows criminal networks to scale up the scope, precision, and efficiency of their operations and is rapidly lowering the barriers to entry for new criminal networks to enter the scene.[3] Recent findings from the UN Office on Drugs and Crime (UNODC) reveal a 600% surge in AI-generated deepfake content linked to fraud in Southeast

Asia in early 2024, underscoring the rapid adoption and increasing role of advanced technology in these crimes.[4]

The most common type of online scam associated with the scam centers or compounds in Southeast Asia is the one commonly referred to as "pig-butchering". This term refers to the practice of grooming targets, or "fattening them up" before extracting the maximum financial value from them, or "slaughtering".[5] These scams are mainly a form of investment fraud, whereby targets are persuaded to invest in seemingly lucrative opportunities. Sometimes there are also elements of a romance scam, where targets unknowingly enter an online romantic relationship or dynamic with a scammer. There are other variations too; impersonation scams similarly pursue a financial outcome, but rather than pose as a love interest the scammer impersonates a family member[6] or an authority figure such as law enforcement or a government official. Some scammers use phishing or malware to access their victims' information. Most operations are prolonged, and scammers try to retain the same victim for a long time in order to extract the maximum funds possible.




*Source: United Nations Development Programme (UNDP), Anti-Scam Handbook, UNDP Global Centre for Technology, Innovation and Sustainable Development, accessed August 7, 2025, https://www.undp.org/policy-centre/singapore/publications/anti-scam-handbook.*

## WHY ARE SO MANY SCAM CENTERS LOCATED IN SOUTHEAST ASIA?

The relatively recent rise of cyber fraud compounds can be traced to the disruption of Southeast Asia's gambling sector and Chinese criminal networks around the time of the COVID-19 pandemic. As research conducted by the US Institute for Peace (USIP) in 2024[7] outlines, these criminal organizations had invested billions in developing extensive casino and hotel complexes throughout Southeast Asia, anticipating significant tourism revenue and profits. When pandemic restrictions halted international travel and casino operations, these criminal enterprises strategically repurposed this infrastructure for cyber-enabled fraud operations to maintain their income. This adaptation wasn't driven by the physical infrastructure itself but by a calculated market response. Additionally, COVID-19 travel restrictions in 2020 resulted in the departure of many Chinese expatriates, further straining traditional revenue streams. Consequently, these scam centers have rapidly evolved into extensive complexes with a growing global reach, with victims of more than 40 nationalities trafficked into these compounds, highlighting the international scope of this crime.[8] This expansion is not limited to Southeast Asia, as these operations are increasingly extending into regions like Africa and Latin America, indicating a growing global footprint.[9]

## WHO IS BEING HARMED?

Scams harm both the individual forced to work in the scam centers and compounds as well as the individuals and communities on the receiving end of scams. The number of affected individuals grows constantly, but it has been difficult to measure and quantify the impact as affected countries track fraud through reporting centers and metrics that vary from country to country, or that do not yet distinguish cyber-enabled fraud from other forms of fraud or cybercrime. A lot of cyber-enabled fraud and scamming goes unreported because victims feel shame or embarrassment, or do not have clarity on who to report it to. Yet growing interest in the issue is driving reporting and tracking. In 2024, cybercriminals earned an estimated USD 1.03 trillion from online scam operations.[10] Between 2020 and 2024, an analysis of fraudulent cryptocurrency wallets estimated about $75 billion as the revenue from 'pig butchering' alone.[11] In 2024, the FBI's Internet Crime Complaint Center report showed losses from cryptocurrency-enabled investment fraud totaled over $6.5 billion.[12] Key U.S. allies, partners, and markets have

likewise been affected at similar levels and have accounted for this emerging, multifaceted threat in their annual national strategies for cybersecurity.

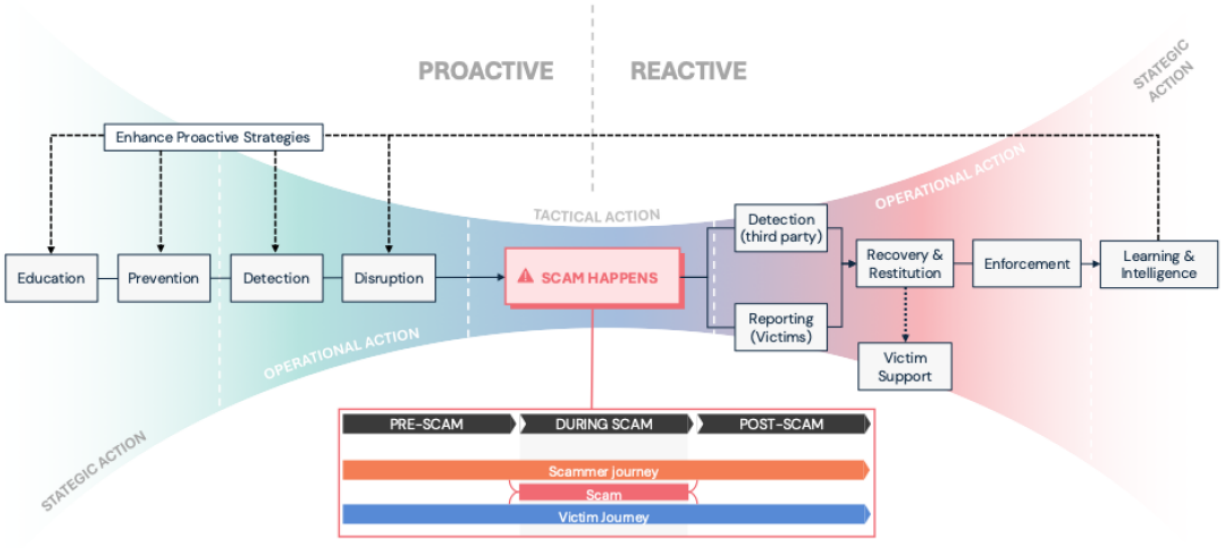
## Mapping the Response

Online scams are a complex, fast-moving and multifaceted problem. National governments and other actors were initially slow to respond, but efforts are starting to gain traction. One of the primary challenges for countering online scams is that there is no single agency, community, or sector that can address this problem alone. Not only is it transboundary but it also sits at the intersection of other transboundary threats: organized crime, money laundering, human trafficking, and corruption. While there are legal frameworks addressing many of these issues, the way in which they intersect and unevenly apply to online scams makes it challenging to pursue and bring down scam operators. There are confusing and inconsistent terminologies being used ("internet fraud" "online scams" "cyber scams") and associated concerns over the role and responsibility of private sector actors such as social media platforms, satellite internet providers, banking and financial services, and telecommunications providers. The law enforcement communities who track more traditional forms of transnational crime do not always have the capacity, training or tools to investigate and respond effectively. It is not a typical 'cybercrime' akin to ransomware, for example, nor is it fraud in the traditional sense because of its digital/cyber-enabled dimension. Reporting rates are uneven and not centralized, and conceptualizations of who is a victim vary and have been politicized.

These unique and overlapping challenges therefore require coordinated response: globally, regionally, nationally and with a wider ecosystem of actors such as banks, cryptocurrency companies, social media corporations, civil society actors, and law enforcement agencies.

To effectively combat this evolving threat, a multi-faceted and globally coordinated approach is essential, encompassing actions like easy national-scale online reporting, the establishment of a global fraud data-sharing hub, and measures to hold service providers responsible and liable. Such recommendations, as put forth by the Global Anti-Scam Alliance,

demonstrate the variety of strategies needed to 'turn the tide' on scams and mitigate the devastating impact of cyber-enabled fraud on individuals, economies, and global security.[13]




*Source: United Nations Development Programme (UNDP), Anti-Scam Handbook, UNDP Global Centre for Technology, Innovation and Sustainable Development, accessed August 7, 2025, https://www.undp.org/policy-centre/singapore/publications/anti-scam-handbook.*

This explainer presents an overview of national government responses to online scams from Australia, Canada, the Philippines, Singapore, Thailand, the United Kingdom (UK) and the United States (U.S). It considers if the country has established a specialized agency, center, or other body, including for reporting scams; relevant laws, strategies, and policies including relevant cybersecurity, cybercrime, and fraud policies; actions taken by relevant private sector actors such as telecommunications and banking; international coordination; and public awareness or education. These are not exhaustive studies of each country's response but attempts to capture major lines of effort. Country profiles have been authored by Stimson Center staff and peer reviewed by external experts based in each country. The relevant and important efforts of civil society and international organizations are not studied in this explainer.

| | Australia | Canada | Philippines | Singapore | Thailand | UK | U.S. |
|---|---|---|---|---|---|---|---|
| Establishment of a specialized agency, body, or center for scams and/or online fraud | ✓ | ✓ | | ✓ | ✓ | ✓ | |
| Centralized reporting platform or agency | ✓ | * | ✓ | ✓ | ✓ | ✓ | ✓ |
| Specialized domestic legal or policy frameworks or strategies | ✓ | ** | ** | ** | ✓ | ✓ | ✓ |
| Efforts involving relevant sectors (telecommunications, banking) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| International coordination | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Awareness-raising/public education campaigns | ✓ | | ✓ | ✓ | | ✓ | ✓ |

*An updated and streamlined system to be released in 2025.

**Focused laws or policies on cyber scams are embedded within existing laws or policies, such as on cybercrime or fraud prevention, rather than standalone.

## Australia

Australia has adopted a multipronged response to prevent, disrupt, and mitigate cyber-enabled scams. Some argue that as a result of moving quickly and its multi-pronged approach, Australia has been successful in bringing down the rate of cyber-enabled scams. The primary national institution is the Australian National Anti-Scam Centre (NASC), established as part of the Australian Competition and Consumer Commission (ACCC). The NASC is tasked with three key areas of responsibilities: collaboration (technology and intelligence sharing), disruption, and awareness and protection with the end goal of intercepting contact between scammer and their targets.[14] A hallmark of this multi-pronged approach is NASC's creation of fusion cells and workgroups that bring together digital platforms, telcos, payment service providers, and crypto exchanges. NASC has also developed the Actionable Scam Intelligence Service, enabling "near real-time exchange of scam intelligence to organizations that can block and stop scams".[15] It has also scaled up website takedowns with over 10,000 websites already removed, including investment, crypto, phishing, and online shopping scam sites.

NASC has worked closely with the Australian Cyber Security Centre (ACSC) and the Australian Federal Police (AFP) to ensure coordination and avoid duplication in reporting and response. The AFP-led Joint Policing Cybercrime Coordination Centre (JPC3) has been particularly effective in targeting payment redirection scams and money mules. In parallel, the Australian Communications and Media Authority (ACMA) developed the Reducing Scam Calls and Scam SMS Industry Code (Scam Code), which blocked over 455.9 million scam calls and over 413.9 million scam SMS in 2024.[16]

While the NASC focuses on prevention and disruption, Australian law enforcement works with ASEAN and other partners to trace and prosecute criminal actors. Legal frameworks such as the Cyber Resilience Framework (2023) and the Surveillance Legislation Amendment (Identify and Disrupt) Bill (2020) empower agencies to move quickly against transnational criminals and take down suspicious domains, cryptocurrency wallets, and websites while collecting evidence that can be used for prosecution.[17] More recently, the Scam Prevention Framework (SPF) proposed under the Scam Prevention Bill (2024) united sectoral approaches under a common regulatory umbrella that addresses three sectors: telecommunications services,

banking, and digital platforms including search engines, messaging, and social media. The framework imposes financial penalties for contraventions by regulated businesses and seeks to protect consumers and small businesses from telecoms and cyber scams.[18]

In parallel, the Australian government has strengthened collaboration with telecommunications providers, mandating proactive filtering for scam text messages and blocking international inbound calls that spoof a domestic number.[19] Fake financial ads are also blocked in Australia by requiring financial services advertisers to demonstrate that they are on a government-authorized list.[20] Public awareness has also been prioritized through the national "Fighting Scams" campaign, which educates Australians on identifying, avoiding, and reporting scams across digital platforms.[21] Additionally, in a major enforcement action, Australia recently revoked 95 company licenses for companies suspected of facilitating scam activity, particularly fraudulent investment schemes involving foreign exchange and digital assets.[22] This deregistration comes as part of a broader crackdown on scam-related operations to protect consumers from financial fraud. The Australian Financial Crimes Exchange (AFCX) furthers this protection by providing security capabilities, technology, and intelligence in one central platform. AFCX also runs the Fraudulent Reporting Exchange (FRX) as a safe network that enables financial institutions to efficiently report and address fraudulent activities.[23]

It is important to note that while the 2023-2030 Australian Cyber Security Strategy provides a broad framework for national cyber resilience, its primary focus is on threats like ransomware and data theft. However, several of its "cyber shields", such as strong businesses and citizens, world-class threat sharing, and resilient regional leadership, do support scam prevention through public education, rapid threat disruption, and international cooperation, leading to an additional layer of scam prevention.

Internationally, Australia has invested in forming diplomatic and operational partnerships in the Indo-Pacific over time, leveraging them against transnational cybercrime. For example, the JPC3 partnership between the AFP and local policing subagencies focuses on "high-harm, high-volume"[24] cybercrime. Regionally, Australia coordinates the Pacific Transnational Crime Network and the AFP's largest international presence is in Southeast Asia, with 30 permanent members based in the region.[25] Through these joint and interagency bodies, the Australian Police

launched Operation Firestorm to target cyber scam centers in Southeast Asia and Eastern Europe. As part of this, the Australian and Philippine police forces jointly shut down a scam compound in Manila in October 2024 in which they arrested 250 suspected scammers and collected digital and physical evidence to support arrests and rehabilitate victims in collaboration with international embassies.[26] Additionally, the joint ASEAN-Australia Counter Trafficking Program (ASEAN-ACT) conducted detailed assessments on the state of play of forced criminality and human trafficking for cyber scams in Cambodia and outlined four sets of recommendations for a variety of government and non-government stakeholders.[27]

## Canada

The 2025 Canadian Cybersecurity Strategy recognizes in its section on cybercrime that Canadians report growing losses from cyber-enabled fraud.[28] An estimated $227 million USD ($310 million CAD) was reported lost to investment fraud in 2024, nearly half of the total reported losses of $473 million USD ($644 million CAD). Spear phishing (targeted email scams) and romance scams were also among the top ten frauds reported in 2024.[29] Scam victims and targets come from diverse demographic profiles, including along lines relating to language, ethnicity, or age.[30]

There are two institutions empowered to address and respond to cyber-enabled scams and fraud. The Canadian Anti-Fraud Centre (CAFC), established in 1993, collects information on fraud and identity theft.[31] Its website includes extensive information about a wide range of fraud types that affect businesses and individuals alike and in recent years has incorporated information on romance and crypto scams, which are prevalent in Canada. The CAFC is the central point for reporting cybercrime and fraud, allowing individuals to report incidents through their online system or by phone. It also publishes an annual report on fraud statistics[32] and conducts diverse public awareness-raising and education campaigns. The CAFC is s jointly managed by the Royal Canadian Mounted Police (RCMP), the Competition Bureau Canada, and the Ontario Provincial Police.

The CAFC works in tandem with the National Cybercrime Coordination Centre (NC3), established by the Royal Canadian Mounted Police in 2020. NC3 was a response to the rise of

cybercrime in Canada and in line with priorities outlined in the Government of Canada's (former) National Cyber Security Strategy, and the RCMP Cybercrime Strategy.[33] The NC3 consists of police officers and civilians from various backgrounds and areas of expertise. The Centre works with Canadian law enforcement as well as national and international partners to help reduce the threat, impact, and victimization of cybercrime in Canada, including through building capacity. The CAFC and NC3 report to the same Director-General and are both stewarded by the RCMP as part of National Police Services[34].

In 2025, Canada will launch a new cybercrime and fraud reporting system to make reporting easier and more streamlined.[35]

As in other countries, it can be challenging for Canadian victims to seek justice. This is largely because scam centers – and thus, the origin of the crime - are located overseas which creates jurisdictional barriers for investigation and evidence collection. One expert in Canada has additionally noted that losses must reach a certain financial threshold before law enforcement can take up a case. Staffing cybercrime police units adequately has been challenging for particular crime phenomena, and existing staff require training on the tactics and tools being employed in cybercrime, including scams.[36] Canadian privacy laws[37] are intended to protect individuals from harm but sometimes pose challenges for scam prevention or response measures because their emphasis on privacy and consent can complicate the collection and use of information needed for investigations.

Interviews with Canadian stakeholders and experts highlight the growing sophistication of scams, whether due to AI tools or phony websites that look increasingly credible. Victims are increasingly sending money through cryptocurrency transactions, but sometimes, bank-to-bank transactions are used. RCMP can trace fraud wallets and pattern the transactions in cooperation with international partners, based on fraud reports that tell RCMP what wallets victims used to send cryptocurrency to and tracing of the transactions to that wallet. Project Altas, an initiative of the Ontario Provincial Police, is an example of this type of response.[38] Yet the majority of funds lost to crypto scams go unrecovered often because the funds were routed through unscrupulous or foreign exchanges or were converted back into traditional currency to prevent the cryptocurrency exchange from accessing the funds.[39]

The Canadian Telecommunications Association's website outlines several measures it has in place to help prevent fraud.[40] This includes Universal Network-Level Call Blocking (UNLCB), which blocks calls with blatantly false call display data. Calls with invalid numbers are automatically blocked, such as numbers like 000-000-0000 and others that don't conform to international numbering plans. Caller ID Authentication (STIR/SHAKEN) protocols help protect Canadians from spoofed calls by verifying the authenticity of caller ID information. These protocols use digital certificates to confirm that a call is coming from the displayed number and has not been altered in transit. Telecom providers also use various spam filters to protect consumers from unwanted text messages and emails. Major Canadian banks also offer guidance and have implemented various safeguards against scams and fraud, in cooperation with major credit card companies, and have obligations to work with relevant government agencies and offices.[41]

## Regional Context: China/Myanmar

*Unlike the country profiles, this section contextualizes the problem of scams within China-Myanmar relations. It is drawn from a commentary originally published by Sydney Tucker of the Stimson Center's Myanmar Project in April 2025.*[42]

China's approach to addressing online scams is shaped both by the rise of scam centers in neighboring Southeast Asian countries targeting Chinese citizens and by the impact these operations have on its relationship with Myanmar.

As a previous Stimson commentary, *Cyber Scam Centers: A Growing Flashpoint in China-Myanmar Relations,*[43] lays out, scam centers are often located along the China-Myanmar and Thailand-Myanmar borders. They have increasingly become a concern for China due to the role of human trafficking and forced labor in the centers, and because of impacts on Chinese citizens as both trafficking and scam victims. This issue gained prominence in late 2023, coinciding with a broader deterioration in Myanmar's internal stability and the rise of public pressure in China to address scams. China has shifted its stance toward Myanmar multiple times, initially backing the junta to prevent state collapse, but later distanced itself due to the junta's failure to control border security and transnational crime, while still engaging diplomatically to

preserve its strategic interests. China's de-facto support of the October 2023 Operation 1027 offensive - an ongoing military operation led by the Three Brotherhood Alliance (3BA) - was partly owing to the Alliance's support for cracking down on scam centers. Their success in doing so forced many of the centers further south. While this has moved the problem away from China's border, it has not stopped the trafficking of Chinese citizens.

Public outcry intensified after the abduction of Chinese actor Wang Xing in January 2025.[44] His abduction and rescue raised question on the extent to which the Chinese government is involved in these operations. A grassroots movement titled "Stars Go Home Plan" began tracking Chinese victims of scam compounds and was quickly censored by the Chinese government.[45]

China's President Xi Jinping and Foreign Minister Wang Yi have been vocal about the threat posed to both Chinese citizens and the overall stability of a region by these scam centers.[46] They have also praised the efforts of the Thai government and others in the region in shutting down scam operations. Rhetorical statements have been met with action, such as a joint Thai and Chinese coordination center as well as the largest repatriation of 200 cyber scam suspects back to China in February 2025.[47]

Despite these efforts, scam operations continue to shift geographically, moving further from China's immediate border and making their efforts to contain these operations far more difficult, especially in areas of Myanmar junta's control. China has continued its efforts to use diplomatic clout and pressure to incentivize the prosecution and shutting down of cyber scam operations for the sake of the wellbeing of Chinese citizens as well as broader regional stability.

## Philippines

Fraud and online scams have been an ongoing challenge in the Philippines for many years, but the issue was exacerbated significantly due to rapid digitalization during the COVID-19 pandemic, particularly the rise in online banking and the use of other online payment apps and services. In early 2024, the Philippine National Police (PNP) announced a more than 20% year-on-year increase for cybercrimes, particularly scams in online marketplaces, investment

scams, and credit card fraud.[48] A survey by the Global Anti Scam Alliance (GASA) indicated that two-thirds of individuals surveyed encounter scams at least once a month, and that scam losses reached approximately $8.1 billion USD in 2024 (about 2% of the Philippines' GDP).[49]

## CYBERSECURITY AND CYBERCRIME FRAMEWORKS

In February 2024, the government announced the National Cyber Security Plan 2023-2028 which broadly aims to proactively protect and secure cyberspace in the Philippines and includes a variety of actions and policy framework pathways to improve cyber security defense strategies.[50] Scams are mentioned a few times, notably within the context of efforts to harden telecoms management including the threats of SMS scams, spam, and phishing. Two other related acts related to money mule accounts and blocking of online websites related to piracy have been proposed; one has passed (see AFASA section below), the other is still under discussion.[51]

The Cybercrime Prevention Act of 2012 (Republic Act 10175) established a legal foundation for addressing cybercrime. It identified a concrete definition and list for cybercrime acts, relevant penalties for such acts, and mandated the creation of specialized cybercrime units within the National Bureau of Investigation (NBI) and the PNP, as well as an Office of Cybercrime within the Department of Justice (DOJ).[52]

The Cybercrime Investigation and Coordinating Center (CICC) is the lead agency for implementing the Cybercrime Prevention Act of 2012. It is responsible for monitoring and preventing cybercrime; facilitating international cooperation coordinating with government agencies, the private sector, and NGOs; and recommending legal updates.[53] The CICC operates as an attached agency under the Department of Information and Communications Technology (DICT) and collaborates with the National Privacy Commission (NPC), and National Telecommunications Commission. Under the Cybercrime Prevention Act, the CICC can request support from key agencies including Immigration, Drug Enforcement, Customs, National Prosecution, Anti-Money Laundering Council, Securities and Exchange Commission, and other relevant organizations. This structure acknowledges that cybercrimes frequently involve financial systems, cross-border activities, and established criminal networks.

The Senate is considering potential amendments to the Cybercrime Prevention Act to update it given the current situation in the Philippines with higher levels of internet users and devices,the increasing sophistication of criminal actors, as well as the widespread emergence of online scams as the most prevalent type of cybercrime. Senate Bill 2570[54]–proposed in February 2024– would grant the CICC greater mandate to coordinate on cybercrime prevention and investigation, ensuring the implementation of updated cybercrime laws, and integrate additional service providers into the prevention efforts. Additional laws under consideration are outlined here.[55]

## PRIVATE SECTOR REGULATION

There are also specific regulations and laws passed to address fraud and scams within the financial sector. In 2022, the central bank of the Philippines, Bangko Sentral Ng Pilipinas (BSP), provided a circular memo requiring fraud management systems and consumer awareness efforts on the part of financial institutions it oversees.[56] In July 2024, the government passed the Anti-Financial Account Scamming Act (Republic Act 12010, also known as AFASA) which aims to specifically outlaw and provide punishment for financial crimes including but not limited to operating money mule accounts, performing fraud or scams via social engineering, and other similar crimes.[57] AFASA allows the BSP to investigate such crimes related to bank accounts, e-wallets, or other financial accounts and mandates additional responsibilities for financial institutions to implement a fraud management system.[58]

## PUBLIC AWARENESS AND REPORTING

Public awareness is a cornerstone of the Philippines's strategy to combat online scams and broader cybercrime. The government has significantly expanded its cybersecurity education and reporting mechanisms. In 2024, the DICT launched a cybersecurity awareness campaign as part of the National Cybersecurity Plan 2023-2028.[59] The DICT regularly publishes updates on emerging scam tactics and cybersecurity tips, in combination with capacity-building initiatives. In the case where fraud does happen, the Philippines has numerous lines to report it. The primary official reporting channel runs through the Inter-Agency Response Center (I-ARC) via Hotline

1326, which is run by a consortium of DICT, CICC, NPC, and NTC with NBI and PNP support.[60]

## Singapore

International scamming of Singaporean citizens has been a major issue in recent years, with the number of reported crimes increasing nearly 50% annually most years since 2019.[61] Singapore's advanced digital infrastructure and relatively high digital connectivity rates make it a target for online scams. However, this has prompted a robust and complex response which includes significant regulatory and legislative efforts, law enforcement initiatives, and government engagement with telecommunications companies and banks, among other actors.

### LEGISLATIVE RESPONSE

There are different laws within Singapore that collectively provide a foundation for pursuing scammers and/or individuals that support them (i.e. money-mules). The 1993 Computer Misuse Act inhibits the use of computers or digital accounts for unauthorized or illegitimate access to programs or data.[62] The Corruption, Drug Trafficking, and Other Serious Crimes Act of 1992 applies to money laundering[63]. New sentencing guidelines updated both laws to cover offenses such as providing scammers with account credentials for use in scams as well as money.

The Penal Code 1871, particularly Section 420, is used to prosecute scam-related offenses involving cheating or deceiving someone in order to deliver property with value[64]. This section includes terms of up to ten years and potential fines and was last amended in 2021. The 2019 Payment Services Act provides a framework for regulating payment systems and services in Singapore and has particular relevance to digital payments and financial tech companies which are often utilized to pass funds by scammers and scam victims. In 2024 the Monetary Authority of Singapore issued a circular with guidance on adoption of anti-scam measures by institutions that are licensed under the Payment Services Act and which are raising the cap for e-wallets.[65]

In 2023, Singapore passed the Online Criminal Harms Act, which allows for directives to online service providers or other entities when there is suspected scam activity and mandates

providers to establish systems or measures to counter such offenses or fix vulnerability points.[66] Building on this Singapore's government passed the Protection from Scams Bill in early January 2025, which allows the police to order banks to unilaterally halt banking transactions for individual accounts to prevent victims from transferring funds to scammers and to extend such restriction orders for up to six months.[67] It entered into force on July 1, 2025. The Act recognizes that in many cases where there is significant financial loss, the victims willingly authorized the transfer of funds because of fraudulent actions of the scammers (such as through government impersonation or romance and investment scams).

Aspects of the 2024 Law Enforcement and Other Matters (LEOM) Bill seeks to deter the misuse of local SIM cards for criminal activities including scams by introducing penalties for errant subscribers, middlemen, and retailers[68]. According to the Ministry for Home Affairs, the number of local mobile lines involved in scams and other cybercrimes had quadrupled from 2021 to 2023 in an effort to get around measures introduced in 2022 to block overseas scam calls and text messages.[69]

## ANTI-SCAM COMMAND AND LAW ENFORCEMENT

The creation of the Singapore Anti-Scam Command (ASC) in 2022 was a significant step forward to coordinate national efforts and has underpinned more recent legislative and implementation efforts. The center sits within the Singapore Police Force. Its work is predicated across six lines of effort: information management; intervention; deterrence; coordination with external stakeholders; public awareness raising; and international cooperation.

Given the nature of online scam strategies and operations, the ASC partners with more than 80 outside institutions to counter online scams.[70] Importantly, key technical experts from other government agencies as well as staffers from key banks and other services are seconded to the ASC. This allows them to respond rapidly and in real-time to investigations, helping to trace funds and freeze bank accounts involved with scams and fraudulent fund transfers.

## BANKING INITIATIVES

In mid-2022, the Monetary Authority of Singapore along with the nonprofit industry group the Association of Banks in Singapore adopted a series of measures to help prevent losses,

including a temporary self-service suspension of an account to prevent transfers (often called a "kill switch"), a locking feature to set aside certain funds which are not eligible for transfer, and instituting a default daily withdrawal limit for online withdrawals to avoid rapid draining of accounts. This was essentially required by banks operating in Singapore, although individual banks implement the "kill switch" differently.[71] Another measure is the imposition of a 12-hour "cooling-off period" in which a transaction that is deemed "high risk" will not be available when an account is set up on a new device.[72] Since 2022, there have been efforts to require facial verification for high-risk transactions using Singpass, a trusted digital ID program. Since 2023, the government has increased coordination with banks on additional preventative measures such as blocking account access from devices which give indications of malware infection.

## INFORMATION AND TELECOMMUNICATIONS INITIATIVES

The Infocomm Media Development Authority (IMDA) of Singapore leads engagement on digital economy and society in Singapore, and has been responsible for coordinating with telecommunications companies to limit scammer access.[73] Since 2017, IMDA implemented progressive anti-spoofing measures: verification processes (2017), blocking spoofed numbers and malicious SMS links (2019), robocall pattern recognition (2020), blocking international calls with domestic numbers and SMS scanning (2022), and mandatory sender ID registration with "likely SCAM" tags (2023).[74] Results show a 97% reduction in calls spoofing Singapore's +65 country code through Q3 2023, with two-thirds of remaining calls identified and blocked as spam.[75]

In support of these efforts, the Singaporean government worked with the private sector to develop Scamshield, an app which they advocate for citizens to install on their phones to block and filter robo- and overseas calls, track and blacklist bad actors, and/or double check if a link or message is a scam[76]. The government also established a public awareness campaign, ACT Against Scams, which encourages users to "Add" security measures (like Scamshield or banking verification steps), "Check" for potential signs of scams, and "Tell" the authorities about any suspicious activity.[77]

## Thailand

Thailand faces a severe scam epidemic. According to a 2024 Global Anti Scam Alliance survey, nearly 90% of Thai citizens encounter scams monthly, with 60% reporting increased exposure compared to previous years. [78] The financial impact is significant, with average losses of $1,100 per person in 2024—a $150 increase from 2023 and a substantial burden given Thailand's GDP per capita of approximately $7,182.[79]

In response the government has adopted a multi-faceted approach which combines legislation, institutional cooperation, technological measures, and cross-border enforcement to combat the growing threat of scams targeting its citizens.

### INSTITUTIONAL FRAMEWORK

The foundation for Thailand's anti-scam infrastructure began in 2020 when the king passed a Royal Decree creating the Cyber Crime Investigation Bureau (CCIB) within the Royal Thai Police.[80] This specialized unit is responsible for preventing and investigating technological crimes, establishing operational procedures, and supporting evidence analysis for cybercrimes. Additionally, the Royal Thai Police Royal maintains a Technology Crime Suppression Division within the Central Investigation Bureau, and the Department of Special Investigation has its Bureau of Technology and Cyber Crime.[81]

In November 2023, multiple government agencies launched the Anti-Online Scam Operation Centre (AOC) as a centralized reporting mechanism. The AOC operates a national hotline (1441) for citizens to report scams and seek information. It coordinates across financial agencies to freeze and track funds following scam reports.[82]

The Securities and Exchange Commission also established an Investment Scam Hotline in collaboration with the AOC and partnered with popular messaging platforms like Meta and LINE to block fraudulent activities.[83] In January 2025, the Royal Thai Police created a "War Room" at headquarters integrating True Corporation (a major telecom provider) to analyze SMS and call patterns.[84]

## LEGISLATIVE RESPONSE

In 2023, Thailand enacted the Emergency Decree on Technological Crime Prevention and Suppression[85] to specifically address electronic and telecommunications fraud. Key provisions include:

- Requiring financial institutions and telecom operators to disclose transaction information when fraud is suspected
- Mandating responses to law enforcement information requests
- Enabling seven-day suspensions of potentially fraudulent transactions
- Criminalizing the provision of "mule accounts" with imprisonment and fines

A dedicated Commission will oversee implementation during the decree's five-year term, after which the Ministry of Digital Economy and Society (MDES) and Royal Thai Police will evaluate its effectiveness.[86]

In late 2024, the MDES proposed amendments[87] to strengthen the decree by:

- Streamlining processes to refund victims when funds are frozen
- Increasing service provider responsibility when compliance failures contribute to losses
- Significantly increasing penalties for fraud involvement

These amendments received Cabinet approval in January 2025. In April 2025, the Thai Cabinet approved amendments to two existing emergency decrees to account for the growing threat of online fraud and cybercrime. The Emergency Decree on Measures for the Prevention and Suppression of Technological Crimes (No. 2) B.E. 2568[88] enhances online safety to address scams and digital fraud. The Emergency Decree on Digital Asset Businesses (No. 2) B.E. 2568[89] focuses on cryptocurrency markets to improve regulatory oversight of digital asset service providers.[90]

## PREVENTATIVE BANKING PRACTICES

Following the 2023 Royal Decree, the Thai Bankers Association and Bank of Thailand launched the Central Fraud Register system in August 2024[91] to facilitate information sharing about suspected fraud.[92] Beginning March 2025, the Bank of Thailand has expanded anti-mule

account measures[93] by adding risk levels, enhancing freeze measures, and requiring banks to block transfers to/from identified mule accounts, among other measures.[94]

### TELECOMMUNICATIONS ENFORCEMENT

The National Broadcasting and Telecommunications Commission (NBTC) has implemented measures to limit access to "mule" SIM cards used by scammers.

One key effort was to do a review of all SIM card registrations, requiring people who registered between 6-100 SIM cards to update and verify identify information by mid-2024 or risk suspension and then termination of services.[95] By mid-2024, the NBTC had suspended more than 3 million SIM cards.[96] Other efforts to halt access are linked to identification and blocking of malicious or misleading links and websites for casinos, cryptocurrency investment, or other common avenues for scams.[97]

Thailand also has a unique role given its geography, as Thailand has numerous cross-border lines in the border regions to provide internet, electricity, and in some cases fuel to neighboring communities. There are numerous online scam operation compounds located along the Thai-Myanmar or Thai-Lao borders, and many can access these resources either through legal or illegal connections. For example, the NBTC and Royal Thai Police cracked down on telecom towers at nearly 1,000 locations in 2024, disconnecting signals, adjusting antenna direction to limit services across the borders, and demolishing others.[98] In February 2025, the government of Thailand announced broad cutoffs of electricity, fuel, and internet to key areas suspected of hosting scam compounds with only a day of official lead time before the bans go into effect.[99] The threat was carried out but at least one scam operation remained operational, leaving the situation ongoing. Reports published in June 2025 indicate that authorities are considering extending such measures or targeting additional essential services.[100]

## United Kingdom

It is estimated that 76% of fraud cases in the United Kingdom (UK) now originate online, largely driven by lower-value scams like purchase fraud that accounts for 29% of total financial losses.[101] The national response has focused on disrupting every stage of the “cyber fraud life

cycle".[102] This includes proactive detection and takedown of digital threats as well as close collaboration with financial institutions and technology companies to block fraudulent transactions and dismantle criminal networks.

The UK's response strategy has emerged in recent years in tandem with the spike of cyber-enabled fraud. One 2021 study of British response to scams noted that responsibility for tackling the issue was unclear, creating a policy "leadership vacuum" and leaving financial institutions as the first line of defense in any instance of cyber fraud and in which UK law enforcement agencies were overburdened and under-resourced to meet the growing number of victims.[103] Since then, the government has taken steps to centralize leadership and expand operational capacity.

In 2023, the UK passed the Online Safety Act (OSA) and announced a national Fraud Strategy aimed at reducing fraud by 10% by the end of 2024.[104] The OSA introduced new legal duties for online platforms to assess and mitigate the risk of fraudulent content, including scam ads and impersonation attempts. Regulated services are now required to implement systems for detecting and removing fraudulent material, verifying advertisers, and cooperating with law enforcement.[105] Ofcom, the UK's communications regulator, is responsible for enforcing these provisions and has begun issuing codes of practice to guide compliance.[106]

The Fraud Strategy expanded the role of the National Cyber Security Centre (NCSC), originally established in 2016 under the British National Cyber Strategy 2016-2021. The NCSC is the UK's central incident response body for cyberattacks, playing a role in fraud prevention through intelligence sharing, technical disruption, and public reporting tools.[107] The NCSC launched the "Share and Defend" hub, a national platform for threat intelligence sharing between government, law enforcement, and industry to proactively disrupt scam operations.[108]

To strengthen investigative capacity, the government established the National Fraud Squad, a specialized unit tasked with targeting the most complex and high-value fraud operations. Action Fraud, the National Fraud and Cyber Crime Reporting Centre established in October 2009 now operated by the Home Office, has yet to see its promised replacement, despite the National Fraud Squad beginning operations. Action Fraud remains in use despite longstanding criticism for being outdated and ineffective.[109] The government has committed to

launching a new, state-of-the-art reporting platform, but delays have hindered progress, resulting in a critical gap in both victim support and reliable data collection.

The Joint Fraud Taskforce (JFT), originally established in 2017, was relaunched in 2021 with a renewed mandate to coordinate cross-sector efforts to combat fraud.[110] Chaired by the Minister for Fraud and housed within the Home Office, the JFT brings together law enforcement, government, and private sector leaders to implement sector-specific fraud charters and drive collective action.[111] It also monitors progress on national fraud reduction targets and facilitates data sharing across industries.

Despite these efforts, challenges remain. Some experts note that longstanding issues such as fragmented leadership, limited digital forensics resourcing, and continued delays in replacing Action Fraud have undermined the effectiveness of national strategies.[112] Only 14% of fraud cases are reported to Action Fraud or the police by victims, further demonstrating the public's lack of confidence in the existing system and the broader tendency to not report which is also found in other countries.[113]

To expand public engagement and prevention, the UK launched the National Campaign Against Fraud in February 2024. The campaign partnered with 30 key stakeholders like the National Crime Agency, the NCSC, and companies like X (formerly Twitter) and Google, and uses television and social media advertising to promote public awareness.[114] The private sector has also taken on a more active role by creating the industry-led membership group Stop Scams UK representing the banking, telecommunications, and technology sectors. Stop Scams allows these sectors to collaborate rather than compete by overcoming regulator, data privacy, and legal obstacles. It also offers free public services to report and prevent fraud, including a phone service for consumers to verify potentially fraudulent calls or messages.[115]

As part of its international efforts to combat cybercrime originating abroad, the UK hosted the inaugural Global Fraud Summit in March 2024, convening G7 and Five Eyes partners to develop a unified approach to tackling cyber fraud. The British Home Secretary and Security Minister, who oversee the JFT, led the summit in collaboration with G7 and Five Eyes partners. The parties endorsed a joint communique advancing a four-part framework to tackle cyber fraud, focusing on enhancing partnerships with the private sector. The framework includes a roadmap

for building international partnerships and capabilities, empowering victims to overcome the stigma associated with fraud and recover lost assets with the help of the Financial Action Task Force (FATF), tackle transnational organized crime actors, and disrupt the ability of scammers to target victims online.[116]

## United States

Scams and cyber fraud have skyrocketed in the United States in recent years, with reported losses quadrupling between 2020 and 2024. Fraud accounted for a majority of reported losses in 2024, which reached a record-setting $16.6 billion.[117] The United States government employs a multi-faceted approach to counter cyber scams and fraud, combining regulatory frameworks, law enforcement efforts, and proactive prevention measures. While these are outlined below, currently no single agency is mandated to coordinate efforts to address cyber scam responses or support victims.

Several federal laws and agencies form the backbone of the U.S. regulatory response to cyber scams. Agencies like the Federal Trade Commission (FTC), Federal Bureau of Investigation (FBI), and Federal Deposit Insurance Corporation (FDIC) regularly issue alerts and provide consumer advice on how to recognize and avoid various types of scams, including phishing, tech support scams, and fraudulent job postings.

The FTC is the primary agency for consumer protection in the United States, enforcing laws that prevent deceptive and unfair business practices. The Fraud and Scams Reduction Act of 2019 specifically tasks the FTC with raising awareness, identifying, and combating schemes to defraud consumers, including the creation of an Office for the Prevention of Fraud Targeting Seniors.[118] The FTC actively disseminates educational materials and logs complaints through its website. And the Federal Communications Commission (FCC) has sought to combat spoofed calls through adopting caller ID authentication (STIR/SHAKEN) in 2021 to identify legitimate calls and mitigate malicious robocalls.[119]

The Department of Justice, particularly through its Computer Crime and Intellectual Property Section (CCIPS), is responsible for investigating and prosecuting a range of

cybercrimes including scams. The Computer Fraud and Abuse Act (CFAA) is a foundational federal law used to prosecute unauthorized computer access, data theft, and other cyber offenses. The FBI, as the lead federal agency investigating cyberattacks, operates cyber squads in its field offices and works with international counterparts. The FBI manages the Internet Crime Complaint Center (IC3), which collects reports of internet crime from the public, publishes annual reports highlighting the state of cyber-crime in the United States, and helps in freezing funds for victims.

In addition to these domestic efforts, the U.S. also works with a wide range of actors internationally to address cyber-scams and fraud. The Department of State's Bureau of East Asian and Pacific Affairs (EAP) and the Bureau of International Narcotics and Law Enforcement (INL), as well as USAID, have in recent years prioritized countering cyber scams originating in Southeast Asia through forming working groups and sharing information about cyber-scams collected from embassies and consulates with other agencies. The U.S. Department of the Treasury has applied Global Magnitsky sanctions three times against individuals enabling or running large-scale cyber scam operations. In 2018, the Golden Triangle Special Economic Zone located in Bokeo Province and its owner Zhao Wei were sanctioned.[120] In 2024 Ly Yong Phat, a Cambodian tycoon with ownership of properties and scam compounds where cyber scams emanate, was sanctioned,[121] and in 2025 warlord Saw Chit Thu, his two sons, and the Karen National Army which he oversees were sanctioned for facilitating cyber scams.[122]

The Trump Administration reportedly has placed countering cyber scams at the top of its Southeast Asia policy priorities, but a comprehensive approach has yet to coalesce. It is unclear whether a Biden Administration inter-agency working group on cybercrime led by the National Security Council's Office of Cyber Policy will continue, and reductions of personnel and resources at many federal agencies which previously funded investigative and enforcement efforts against cyber scams will likely hamper efforts.

Given the rapid proliferation of cyber scams and fraud and the technical nature of the crime, it can be difficult for many victims to recover losses or seek justice. Local law enforcement agencies often lack resources to aid victims of cyber scams and have in some cases told victims that they do not have the capacity nor jurisdiction to process crypto-currency related

scams or crimes. To assist scam victims, promote awareness, and provide guidance on countering the cyber-scam threat, non-government efforts such as Operation Shamrock and the Stop Scams Alliance have been established in recent years.[123] But these organizations have limited resources and access to tackle the issue.

Many social media and messaging platforms such as Meta (Facebook, WhatsApp, Instagram, and Messenger) on which cyber criminals prey on victims are registered or headquartered in the United States. While most of these companies police cyber scam activity, critics argue that they do so in a shallow way despite pledges to increase monitoring and security measures to prevent cyber-enabled crimes. A May 2025 investigation by Wall Street Journal indicates that nearly half of all scam complaints tied to Zelle financial transactions were linked to Meta's subsidiaries Facebook and Instagram.[124] These organizations can likely do more to combat scams in the United States if sufficient public or government pressure is applied, as some have adopted additional safeguards in other countries such as the UK.[125]

## Conclusion

This explainer sought to outline the scope and nature of national responses to the rising challenge of online scams in seven countries which have been heavily targeted.

Every country studied has responded in ways that reflect their respective national contexts, political traditions, and existing capabilities. Responses also reflect the multi-faceted nature of the online scams issue, which straddles cybersecurity and cybercrime, fraud, and human rights concerns. Several of the countries surveyed are moving in the direction of establishing focused agencies or other bodies specific to online scams and frauds, often situated within broader anti-fraud efforts. Some are creating specialized policies or laws that tackle discreet aspects of the issue (such as acting as mules for money or SIM cards) or updating existing cybercrime/computer safety laws or anti-fraud strategies. Many have also introduced centralized reporting platforms or agencies, although the extent to which those well-utilized by scam victims varies. Awareness-raising efforts exist but appear to be somewhat limited in their impact and reach.

It is increasingly clear that national governments cannot act alone and must engage with relevant private sector entities such as banks, social media platforms, and telecommunications providers. Each of these entities has a different role to play in scam prevention, whether in flagging/pausing problematic transfers, removing and improving vigilance against false content, or putting in

place technological blocks and fixes. Globally, it is evident that more coordination would be beneficial whether that is in the area of streamlining national law and policy; improving transborder evidence-sharing and law enforcement; or building cohesion in how private sector entities are engaged, notably social media platforms.

Stimson's research process further identified that greater clarity around the role of different actors at local, national and global levels is needed to enhance cooperation and improve relevant law enforcement. More than anything else, political will to stop scams is a key determinant for success.

Future Stimson Center work on this topic will consider how international legal frameworks in the area of cybercrime, anti-trafficking, and anti-money laundering can be better applied and expanded to counter online scams.

---

[1] INTERPOL, "INTERPOL releases new information on globalization of scam centres," June 30, 2025, https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres.
[2] Gary Warner, "Getting a Job in Pig-Butchering," *Darktower*, July 12, 2023, https://getdarktower.com/getting-a-job-in-pig-butchering/.

[3] United Nations Office on Drugs and Crime,"Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape," October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.
[4] United Nations Office on Drugs and Crime, "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia," April 2025, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.
[5] Chainalysis, "The On-chain Footprint of Southeast Asia's 'Pig Butchering' Compounds: Human Trafficking, Ransoms, and Hundreds of Millions Scammed," February 24, 2024. Accessed June 30, 2025. https://www.chainalysis.com/blog/pig-butchering-human-trafficking/

[6] Federal Communications Commission, "'Grandparent' Scams Get More Sophisticated," last modified March 6, 2025, accessed June 30, 2025, https://www.fcc.gov/consumers/scam-alert/grandparent-scams-get-more-sophisticated#:~:text=According%20to%20the%20Federal%20Trade,Help%20You%20Avoid%20Being%20Scammed.
[7] United States Institute of Peace, "Transnational Crime in Southeast Asia," Priscilla A. Clapp and Jason Tower, co-chairs (2024), p. 5-10. https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security.

[8] U.S. Department of State, "Trafficking in Persons Report 2023: Introduction and Additional Pages," June 2023, https://www.state.gov/wp-content/uploads/2023/05/Trafficking-in-Persons-Report-2023_Introduction-Additional-

Pagesv4_FINAL.pdf"https://www.state.gov/wp-content/uploads/2023/05/Trafficking-in-Persons-Report-2023_Introduction-Additional-Pagesv4_FINAL.pdf.

[9] United Nations Office on Drugs and Crime, "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia," April 2025, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.
[10] Sam Rogers, "International Scammers Steal over $1 Trillion in 12 Months in Global State of Scams Report 2024," Global Anti-Scam Alliance and Feedzai, November 7, 2024, https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai.
[11]Griffin, John M. and Mei, Kevin, "How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering," SSRN, February 29, 2024, accessed June 30, 2025, http://dx.doi.org/10.2139/ssrn.4742235.

[12] Federal Bureau of Investigation, "FBI Releases Annual Internet Crime Report," April 23, 2025, https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report.
[13] Global Anti-Scam Alliance, "Turning the Tide on Scams," 2024, https://www.gasa.org/turning-the-tide-on-scams.
[14] BioCatch, "Exporting Safety: What Nations Can Learn from Australia's Efforts to Scam Proof Banking," 2024, https://www.biocatch.com/white-paper/exporting-safety.
[15] Ibid.
[16] Australian Competition and Consumer Commission, "Targeting Scams: Report of the National Anti-Scam Centre on scams data and activity 2024," 2024, https://www.accc.gov.au/system/files/targeting-scams-report-2024.pdf.
[17] Asha Barbaschow, "Australia's 'hacking' Bill passes the Senate after House made 60 amendments," ZDNET, August 24, 2021, https://www.zdnet.com/article/australias-hacking-bill-passes-the-senate-after-house-made-60-amendments/.
[18] Thomas Jones, Matthew Bovaird, Patrick Cordwell, and Julian Ferguson, "Explainer: Australia's New Scam Prevention Framework," Bird & Bird, March 13, 2025, https://www.twobirds.com/en/insights/2025/australia/explainer-australias-new-scam-prevention-framework.
[19] Paul Karp, "Telcos required to block or flag scam texts under Labor crackdown," The Guardian, December 2, 2024, https://www.theguardian.com/australia-news/2024/dec/03/albanese-government-scam-text-message-warnings-telcos-law-change.
[20] Ken Westbrook and David P. Mansdoerfer, "Cyber-Enabled Financial Crime is Surging: How to Fight Back," February 13, 2025, https://www.thecipherbrief.com/column_article/cyber-enabled-financial-crime-is-surging-how-to-fight-back.
[21] Australian Treasury, "Albanese government launches Fighting Scams Campaign," Stephen Jones, January 12, 2025, https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/albanese-government-launches-fighting-scams-campaign.
[22] The Record (Recorded Future News), "Australia Pulls 95 Company License in Scam Crackdown," James Reddick, April 7, 2025, https://therecord.media/australia-pulls-95-company-licenses-scam-crackdown.
[23] "AFCX," accessed June 30, 2025, https://www.afcx.com.au/
[24] Australian Federal Police, "Operation Firestorm to Target Cyber Scammers Cheating Australians," David McLean, August 28, 2025, https://www.afp.gov.au/news-centre/media-release/operation-firestorm-target-cyber-scammers-cheating-australians.
[25] Ibid.
[26] Australian Federal Police, "AFP Partners with Philippine Authorities in Combating Scam Call Centers," November 26, 2025, https://www.afp.gov.au/news-centre/media-release/afp-partners-philippine-authorities-combating-scam-call-centres.
[27] ASEAN-Australia Counter Trafficking, "Human Trafficking and Forced Labour in Cambodia's Cyber-Scam Industry," Legal Support for Children and Women (LSCW), May 2024, https://www.aseanact.org/wp-content/uploads/2024/05/202405-LSCW-Cyber-scams-and-HT-report-design.pdf.

[28] Public Safety Canada, "Canada's National Cyber Security Strategy: Securing Canada's Digital Future," 2025, p. 28, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/ntnl-cbr-scrt-strtg-2025-en.pdf.
[29] Canadian Securities Administrators, "Canadians losing millions to investment scams: CSA, CAFC and RCMP urge vigilance and reporting," March 13, 2025, https://www.securities-administrators.ca/news/canadians-losing-millions-to-investment-scams-csa-cafc-and-rcmp-urge-vigilance-and-reporting/.
[30] Interview with anonymous source, interview by Allison Pytlak, August 2024.

[31] Canadian Anti-Fraud Centre, "Home," accessed June 30, 2025, https://antifraudcentre-centreantifraude.ca/index-eng.htm.
[32] Canadian Anti-Fraud Centre, "Annual Reports," last modified April 4, 2024, accessed June 30, 2025, https://antifraudcentre-centreantifraude.ca/annual-reports-rapports-annuels-eng.htm.
[33] Royal Canadian Mounted Police, "National Cybercrime Coordination Centre," last modified December 9, 2024, accessed June 30, 2025, https://rcmp.ca/en/federal-policing/cybercrime/national-cybercrime-coordination-centre.
[34] Royal Canadian Mounted Police, "National Police Services," last modified November 6, 2024, accessed June 30, 2025, https://rcmp.ca/en/specialized-policing-services/national-police-services.
[35] Royal Canadian Mounted Police, "New cybercrime and fraud reporting system," last modified March 5, 2025, accessed June 30, 2025, https://www.rcmp-grc.gc.ca/en/new-cybercrime-and-fraud-reporting-system.
[36] Catharine Tunney, "Canadian agencies do not have the capacity or capability to police cybercrime: AG," Canadian Broadcasting Corporation, June 4, 2024, accessed June 30, 2025, https://www.cbc.ca/news/politics/cyber-crime-rcmp-ag-1.7223887.
[37] Notably, the Personal Information Protection and Electronic Documents Act and elements of the Canadian Criminal Code; Government of Canada, "Privacy Act," Department of Justice Canada, 2025, https://laws-lois.justice.gc.ca/eng/acts/p-8.6/.; Government of Canada, "Criminal Code," Department of Justice Canada, 2025, https://laws-lois.justice.gc.ca/eng/acts/c-46/.
[38] Dave Charbonneau, "OPP launches 'Project Atlas' to fight cryptocurrency fraud," CTV News, November 21, 2024, accessed June 30, 2025, https://www.ctvnews.ca/ottawa/article/opp-launches-project-atlas-to-fight-cryptocurrency-fraud/.
[39] Paul Northcott, "Police help victims of crypto-fraud get money back," Royal Canadian Mounted Police, May 9, 2022, https://rcmp.ca/en/gazette/police-help-victim-crypto-fraud-get-money-back.
[40] Canadian Telecommunications Association, "Telecom providers' anti-fraud initiatives," accessed June 30, 2025, https://canadatelecoms.ca/consumer_resource/telecom-providers-anti-fraud-initiatives/.
[41] Canadian Bankers Association, "Protecting Canadian from fraud and scams," accessed June 30, 2025, https://cba.ca/article/financialfraudpreventiontips.
[42] Sydney Tucker, "Cyber Scam Centers: A Growing Flashpoint in China-Myanmar Relations," The Stimson Center, April 7, 2025, https://www.stimson.org/2025/cyber-scam-centers-a-growing-flashpoint-in-china-myanmar-relations/.
[43] Ibid.
[44] Tommy Walker, "Chinese Actor's Abduction to Myanmar Sign of Growing Diversity of Scams," VOA News, January 14, 2025, https://www.voanews.com/a/chinese-actor-s-abduction-to-myanmar-sign-of-growing-diversity-of-scams-/7936112.html.
[45] VOA Chinese, "China Vows to Rescue Scam Victims in Myanmar, Crack Down on Cross-Border Criminal Gangs," January 16, 2025, https://www.voachinese.com/a/china-vows-to-rescue-scam-victims-in-myanmar-crack-down-on-cross-border-crimi-nal-gangs-20250116/7938769.html.
[46] Ministry of Foreign Affairs, People's Republic of China, "Xi Jinping Meets with Thai Prime Minister Paetongtarn Shinawatra," February 6, 2025, https://www.fmprc.gov.cn/eng/xw/zyxw/202502/t20250207_11550783.html.

[47] Embassy of the People's Republic of China in Myanmar, "Chinese Embassy in Myanmar: Joint Operations Continue to Crack Down on Telecom Fraud," February 20, 2025, http://mm.china-embassy.gov.cn/sgxw/202502/t20250220_11559581.htm.
[48] Third Anne Peralta-Malonzo, "Cybercrimes up by 20% in 1st quarter of 2024," Sunstar, June 30, 2024, https://www.sunstar.com.ph/manila/cybercrimes-increased-by-20-in-1st-quarter-of-2024.
[49] Sam Rogers, "International Scammers Steal over $1 Trillion in 12 Months in Global State of Scams Report 2024," Global Anti-Scam Alliance and Feedzai, November 7, 2024, https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai.
[50] Republic of the Philippines, Department of Information and Communications Technology (DICT), "National Cybersecurity Plan 2023-2028," February, 2024, https://www.scribd.com/document/725917893/NCSP-2023-2028-FINAL.
[51] The Philippine Star, "Senate urged to pass bill blockingonline piracy sites," November 19, 2024, https://www.philstar.com/business/2024/11/19/2401151/senate-urged-pass-bill-blocking-online-piracy-sites.
[52] Republic of the Philippines, "Republic Act No. 10175: Cybercrime Prevention Act of 2012," September 12, 2012, https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/.
[53] Cybercrime Investigation and Coordinating Center, "Mandate, Powers, and Functions," accessed July 1, 2025, https://cicc.gov.ph/mandate-powers-and-functions/.
[54] Republic of the Philippines, Nineteenth Congress, "Senate Bill No. 2570: An Act Strengthening Cybercrime Prevention Measures, Amending for the Purpose Republic Act No. 10175, Otherwise Known as the 'Cybercrime Prevention Act of 2012,'" February 26, 2024, https://legacy.senate.gov.ph/lisdata/4355139600!.pdf.
[55] Francis Mark A. Quimba, "Shaping the Digital Future: Regulatory Updates from the Philippines," Tech For Good Institute, accessed July 1, 2025. https://techforgoodinstitute.org/blog/expert-opinion/shaping-the-digital-future-regulatory-updates-from-the-philippines/.
[56] Bangko Sentral NG Pilipinas, "Circular No. 1140, Series of 2022: Amendments to Regulations on Information Technology Risk Management," March 17, 2022, https://www.bsp.gov.ph/Regulations/Issuances/2022/1140.pdf.
[57] Republic of the Philippines, "Republic Act No. 12010: Anti-Financial Account Scamming Act (AFASA)," July 20, 2024, https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/2/97690.
[58] Bangko Sentral NG Pilipinas, "BSP Welcomes Passage of Anti-Financial Account Scamming Law," July 20, 2024, https://www.bsp.gov.ph/SitePages/MediaAndResearch/MediaDisp.aspx?ItemId=7179.
[59] Republic of the Philippines, Department of Information and Communications Technology (DICT), "National Cybersecurity Plan 2023-2028," February, 2024, https://www.scribd.com/document/725917893/NCSP-2023-2028-FINAL.
[60] Republic of the Philippines, Philippine News Agency, "Netizens urged to save gov't anti-scam response hotline 1326," August 14, 2023, https://www.pna.gov.ph/articles/1207775.
[61] Singapore Police Force and National Crime Prevention Council, "2023 Annual Scams and Cybercrime Brief (Infographic)," 2024, https://www.scamshield.gov.sg/files/Scams%20and%20Cybercrime%20Briefs/2023_annual_scams_and_cybercrime_brief_infographic.pdf.
[62] Republic of Singapore, Parliament, "Computer Misuse Act 1993," Revised Edition 2020, Singapore Statutes Online, https://sso.agc.gov.sg/Act/CMA1993.
[63] Republic of Singapore, Parliament, "Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992," Revised Edition 2020, Singapore Statutes Online, https://sso.agc.gov.sg/Act/CDTOSCCBA1992.
[64] Republic of Singapore, Parliament., "Penal Code 1871, Section 420: Cheating and Dishonestly Inducing Delivery of Property," Revised Edition 2020, Singapore Statutes Online, https://sso.agc.gov.sg/Act/PC1871?ProvIds=pr420-.
[65] Monetary Authority of Singapore, "Circular on Anti-Scam Measures by Major Payment Institutions Issuing E-Wallets," Circular No. MAS/PD/2024/10/04, October 25, 2024, https://www.mas.gov.sg/-/media/mas-media-

library/regulation/circulars/pd/circular-on-anti-scam-measures/circular-on-anti-scam-measures-by-major-payment-institutions-issuing-e-wallets.pdf.
[66] Singapore Police Force, "Introduction to the Online Criminal Harms Act (OCHA), " July 2023, https://www.police.gov.sg/Advisories/Online-Criminal-Harms-Act/Introduction-to-OCHA.
[67] David Sun, "Singapore passes Bill to control bank accounts of scam victims; law will also cover cheating cases," The Straights Times, January 7, 2025, https://www.straitstimes.com/singapore/politics/singapore-passes-bill-to-control-bank-accounts-of-scam-victims-law-will-also-cover-cheating-cases.
[68] Singapore Police Force, "Misuse of SIM Card Offences," April 2, 2024, https://www.police.gov.sg/Advisories/Crime/Misuse-of-SIM-Card-Offences.
[69] Samuel Devaraj, "New laws punishing misuse of Singapore SIM cards to come into effect on Jan 1,' The Straights Times, December 30, 2024, https://www.straitstimes.com/singapore/courts-crime/new-laws-punishing-misuse-of-local-sim-cards-to-come-into-effect-on-jan-1.
[70] Singapore Police Force, "Opening of Anti-Scam Command Office," March 22, 2022, https://www.police.gov.sg/media-room/news/20220906_opening_of_anti-scam_command_office.
[71] Irene Tham, "What does a bank's 'kill switch' kill? It became a point of contention after a victim lost money," The Straights Times, December 16, 2024, https://www.straitstimes.com/singapore/what-does-the-kill-switch-kill-it-became-a-point-of-contention-after-a-victim-lost-money.
[72] Bryan Tan, Eng Han Goh, and Nicholas Tok, "Singapore to Implement Shared Responsibility Framework for Phishing Scams," Reed Smith LLP, November 1, 2024, https://www.reedsmith.com/en/perspectives/2024/11/singapore-to-implement-shared-responsibility-framework-for-phishing-scams.
[73] Infocomm Media Development Authority, "Annex B: IMDA and Telcos' Anti-Scam Measures," January 4, 2024, https://www.imda.gov.sg/-/media/imda/files/news-and-events/media-room/media-releases/2024/01/opt-to-block-incoming-international-calls/annex-b.pdf.
[74] Ibid.
[75] Ibid.
[76] Singapore Police Force, "ScamShield," accessed July 1, 2025, https://www.scamshield.gov.sg.
[77] Singapore Police Force, "ACT Campaign," accessed July 1, 2025, https://www.scamshield.gov.sg/act-campaign/.
[78] Sam Rogers, "37 Billion Reasons the Citizens of Malaysia, Taiwan, and Thailand Need Better Scam Protection," Global Anti-Scam Alliance, p. 7-8, October 8, 2024, https://www.gasa.org/post/where-did-the-billions-go-in-malaysia-thailand-taiwan.

[79] World Bank, "Thailand: Country Profile," accessed July 1, 2025, https://data.worldbank.org/country/thailand.

[80] Royal Thai Police, "Royal Decree on the Division of the Royal Thai Police Office", September 6, 2020, accessible at https://www.royalthaipolice.go.th/downloads/laws/laws_04_17.pdf.

[81] Please see https://www.coe.int/en/web/octopus/-/thailand for more details.
[82] The Nation Thailand, "Anti-online Scam Centre gets off the ground," November 1, 2023, https://www.nationthailand.com/thailand/general/40032467.
[83] The Securities and Exchange Commission, Thailand, "SEC launches Investment Scam Hotline to protect the public from frauds," November 6, 2023, https://www.sec.or.th/EN/Pages/News_Detail.aspx?SECID=10247.
[84] The Bangkok Post, "True Partners with Police to Combat Call Centre Scams," January 16, 2025, https://www.bangkokpost.com/thailand/pr/2941171/true-partners-with-police-to-combat-call-centre-scams.
[85] The Kingdom of Thailand, "Emergency Decree on Measures for the Prevention and Suppression of Technological Crimes, B.E. 2566 (2023)," March 9, 2023. https://www.mdes.go.th/law/detail/7455-Emergency-Decree-on-Measures-for-the-Prevention-and-Suppression-of-Technological-Crimes--B-E--2566--2023-.
[86] Ibid.

[87] Komsan Tortermvasana, "Decree amended in push to get tougher on cybercrime," The Bangkok Post, November 7, 2024, https://www.bangkokpost.com/business/general/2897633/decree-amended-in-push-to-get-tougher-on-cybercrime.
[88] Royal Thai Government Gazette "The Emergency Decree on Measures for the Prevention and Suppression of Technological Crimes (No. 2) B.E. 2568," 2025, https://ratchakitcha.soc.go.th/documents/67320.pdf.
[89] Royal Thai Government Gazette, "The Emergency Decree on Digital Asset Businesses (No. 2) B.E. 2568," 2025, https://ratchakitcha.soc.go.th/documents/67321.pdf.
[90] Vero Advocacy, "Thailand Enacts New Technology Crime Laws," April 18, 2025, https://vero-asean.com/vero-advocacy-brief-thailand-enacts-new-technology-crime-laws/.
[91] Somruedi Banchongduang, "Banks share data with Bank of Thailand to combat fraudulent mule accounts, " The Bangkok Post, September 2, 2024, https://www.bangkokpost.com/business/general/2858127/banks-share-data-with-bank-of-thailand-to-combat-fraudulent-mule-accounts.
[92] The system seeks to identify and share information across the financial industry about problematic accounts, which are flagged as either black, gray, or brown mule accounts with varying penalties and limitations placed on each account type.
[93] The Securities and Exchange Commission, Thailand, "SEC strengthens measures to combat digital asset ule accounts, elevates blocking the misuse of foreign platforms for money laundering to reduce public harm," April 8 2025, https://www.sec.or.th/EN/Pages/News_Detail.aspx?SECID=11682.
[94] The 2023 Royal Decree also required that when a victim reports an issue, financial institutions must suspend transactions for up to 7 days to review. And finally, it established required penalties for owners of mule accounts (either imprisonment for up to 3 years and/or a fine of up to $8,300). All of these efforts aim to dissuade Thai citizens and others from acting as mules for criminal transactions.

[95] Komsan Tortermvasana, "Multiple SIM owners told to register," The Bangkok Post, February 10, 2024, https://www.bangkokpost.com/business/general/2739726/multiple-sim-owners-told-to-register.
[96] Komsan Tortermvasana, "National Broadcasting Commission suspends 3m suspicious SIM cards," The Bangkok Post, July 16, 2024, https://www.bangkokpost.com/business/general/2830347/national-broadcasting-commission-suspends-3m-suspicious-sim-cards.
[97] For example, the Ministry of Digital Economy and Society (MDES) has taken efforts to block social media pages and websites which are reported for online gambling, fraud, or other illegal activities. During the first quarter of fiscal year 2025 (October to December 2024), MDES blocked more than 52,000 illegal pages, which was a 60% increase from the same period the previous year.

[98] Komsan Tortermvasana, "National Broadcasting Commission suspends 3m suspicious SIM cards," The Bangkok Post, July 16, 2024, https://www.bangkokpost.com/business/general/2830347/national-broadcasting-commission-suspends-3m-suspicious-sim-cards.
[99] The Nation Thailand, "Thailand announces electricity, fuel, and internet cutoff to call center gangs in Myanmar tomorrow," February 4, 2025, https://www.nationthailand.com/blogs/news/policy/40045916.
[100] Thai PBS World, "Thailand Considers Power, Internet Cuts to Combat Call-Centre Scams in Cambodia," June 27, 2025, https://world.thaipbs.or.th/detail/thailand-considers-power-internet-cuts-to-combat-callcentre-scams-in-cambodia/57801.
[101] UK Finance, "Annual Fraud Report 2025," May 27, 2025, https://www.ukfinance.org.uk/system/files/2025-05/UK%20Finance%20Annual%20Fraud%20report%202025.pdf.
[102] Sneha Dawda, Ardi Janjeva, and Anton Moiseienko, "The UK's Response to Cyber Fraud: A Strategic Vision," Royal United Services Institute, February 2021, https://www.cityoflondon.gov.uk/assets/about-us/police-authority/uk-response-to-cyber-fraud-strategic-vision.pdf.

[103] Ibid.
[104] The Government of the United Kingdom of Great Britain and Northern Ireland, Home Office, "Fraud Strategy: Stopping Scams and Protecting the Public," May 2023, https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public.

[105] Ofcom, "Ofcom's approach to implementing the Online Safety Act," October 26, 2023, last updated 30 June, 2025, https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/roadmap-to-regulation.
[106]Ofcom, "Guide for services: complying with the Online Safety Act," February 27, 2024, last updated May 21, 2025, https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/guide-for-services.
[107] Robert Hannigan CMG, "Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre," Royal United Services Institute, February 27, 2019, https://www.rusi.org/explore-our-research/publications/occasional-papers/organising-government-cyber-creation-uks-national-cyber-security-centre.
[108] The National Cyber Security Centre, "Introducing the NCSC's 'Share and Defend' capability," May 14, 2024, https://www.ncsc.gov.uk/blog-post/introducing-share-defend-acd.
[109] Alexander Martin, " Replacement for Action Fraud, UK's cybercrime reporting service, delayed again until 2025," The Record (Recorded Future News), August 5, 2024, https://therecord.media/uk-action-fraud-replacement-delayed-2025.
[110]The Government of the United Kingdom of Great Britain and Northern Ireland, Home Office, "Joint taskforce relaunched to protect against rise in fraud crime," October 28, 2021, https://www.gov.uk/government/news/joint-taskforce-relaunched-to-protect-against-rise-in-fraud-crime.
[111] The Government of the United Kingdom of Great Britain and Northern Ireland, Home Office, "Joint Fraud Taskforce," October 17, 2017, last updated April 4, 2025, https://www.gov.uk/government/collections/joint-fraud-taskforce#:~:text=The%20Joint%20Fraud%20Taskforce%20(%20JFT,a%20priority%20for%20us%20all.
[112] Sneha Dawda, Ardi Janjeva, and Anton Moiseienko, "Rethinking the UK Response to Cyber Fraud: Key Policy Challenges," Royal United Services Institute, 2021, https://static.rusi.org/cyber_enabled_fraud_bp_final_web_version.pdf.
[113] National Crime Agency, "Fraud," accessed July 2, 2025, https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime.
[114] The Government of the United Kingdom of Great Britain and Northern Ireland, "Stop! Think Fraud," accessed July 2, 2025, https://stopthinkfraud.campaign.gov.uk/.
[115] Stop Scams UK, "Our Members," accessed July 2, 2025, https://stopscamsuk.org.uk/about/our-members/.

[116] The Government of the United Kingdom of Great Britain and Northern Ireland, Home Office, "Global Fraud Summit Communiqué," March 11, 2024, https://www.gov.uk/government/publications/communique-from-the-global-fraud-summit/global-fraud-summit-communique-11-march-2024#preventing-the-reach-and-means-of-fraudsters.
[117] Internet Crime Complaint Center, "Federal Bureau of Investigation Internet Crime Report 2024," accessed July 5, 2025, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[118] Federal Trade Commission, "Fraud and Scam Reduction Act," Pub. L. No. 117-103, 136 Stat. 49, Division Q, Title I, §§ 101–122, accessed July 2, 2025, https://www.ftc.gov/legal-library/browse/statutes/fraud-scam-reduction-act.
[119] Federal Communications Commission, "Spoofed Robocalls," last modified June 2024, accessed July 2, 2025, https://www.fcc.gov/spoofed-robocalls.
[120] U.S. Department of the Treasury, "Treasury Sanctions the Zhao Wei Transnational Criminal Organization," January 30, 2018, https://home.treasury.gov/news/press-releases/sm0272.
[121] U.S. Department of the Treasury, "Treasury Sanctions Cambodian Tycoon and Business Linked to Human Trafficking and Forced Labor in Furtherance of Cyber and Virtual Currency Scams," September 12, 2024, https://home.treasury.gov/news/press-releases/jy2576.
[122] Reuters, « US puts sanctions on Myanmar warlord and militia linked to cyber scams," May 6, 2025, https://www.reuters.com/world/us-issues-new-myanmar-related-sanctions-treasury-dept-website-shows-2025-05-05/.
[123] Operation Shamrock, "Our Work," accessed July 2, 2025, https://operationshamrock.org/about/our-work; Stop Scams Alliance, "About," accessed July 2, 2025, https://www.stopscamsalliance.org/about.
[124] Jeff Horwitz and Angel Au-Yeung, "Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook," The Wall Street Journal, May 15, 2025, https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8?gaa_at=eafs&gaa_n=ASWzDAh554ZqFC1AjOzHUA7Pi-lMNzZzVtHnyCKA1OXF9pcvGKfNEMFzfvj57Rjtmz0%3D&gaa_ts=68654c60&gaa_sig=0xyA0gzRUneCW5TboOM_PVpdcAh-WW5yiLi_pJnpPwj4Fl04PtIzQHoTrSmY2j5wa-V2_cYiqn4-vZykC39uUg%3D%3D.
[125] Ronan Harris, "Helping protect people from financial fraud int he U.K.," Google, May 7, 2021, https://blog.google/around-the-globe/google-europe/united-kingdom/helping-protect-people-financial-fraud-uk/.