COMPLY ADVANTAGE®

ComplyAdvantage.com

THE

State of Financial Crime

2026

Contents

01. Spotlight on financial crime

02. Geopolitics and sanctions

03.

Regional regulatory trends

04.

Regulatory themes

Back to beginning

Next section

Spotlight on financial crime

The macroeconomics of modern illicit flows

Financial crime has remained terrifying in its scale, scope, and diversity in 2025. A report issued by the Institute of Internal Controls and Forensic Investigation Professionals (IICFIP) during the year argued – with some skepticism about more modest estimates – that

financial crimes drained between 10–15% of global GDP and generated a "direct loss of trillions of dollars annually."

This, it noted, was a scale that "rivalled the GDP of the world's largest economies" and exceeded "global development assistance many times over."

Another 2025 study, published by Global Financial Integrity (GFI), a think tank, took a similar perspective. GFI researchers estimated that the aggregate annual revenue from ten major categories of transnational crime, including drugs and human trafficking, totalled an extraordinary $12.30–$16.21 trillion – a dramatic escalation from GFI's 2017 estimates of roughly $1.6–$2.2 trillion. One of the reasons for the significant growth in the GFI figures over eight years has been the inclusion of cybercrime in their calculations. GFI researchers estimate that cybercrime alone accounts for between 59% and 75% of the global illicit economy, with a value of $7.3–$12.2 trillion per year.

These stunning figures partly reflect a simple recognition of cybercrime's existence. However, it is not hard to imagine that if GFI had been assessing the scale of cybercrime in 2017, its 2025 figures would still have shown a dramatic increase in its size over the intervening period. Where previously much of the illicit economy was purely physical and cash-based, the emerging ecosystem of transnational organized crime has become increasingly virtual and digital in the 2020s, driven by rapid advances in technology and historical events such as the COVID-19 pandemic, which pushed more people online. By leveraging e-commerce platforms, social media, instant messaging, end-to-end encryption, and, of course, the dark web, criminal networks have discovered that they can operate with high degrees of efficiency, anonymity, and security online. Not only that, but operating online and using automated processes and software also allows them to scale quickly: more bang for their illicit buck.

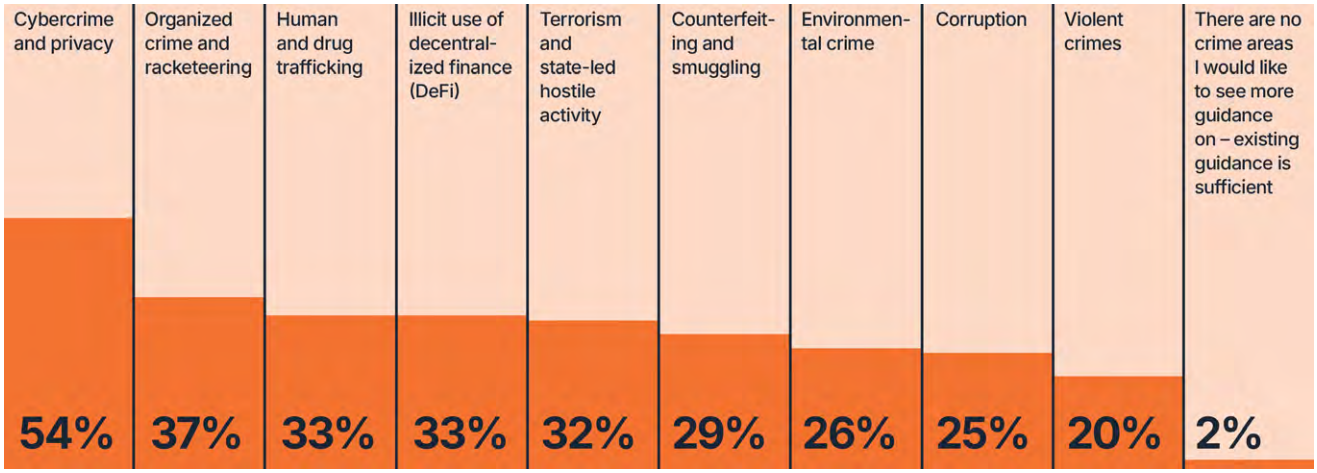
The criminal landscape has undergone a decisive shift. In the EU's Serious and Organized Crime Threat Assessment (SOCTA) for 2025, Europol, the EU's law enforcement agency, notes the rapid pace of change in the criminal world. "Traditional" criminal enterprises, like drug dealing, have increasingly moved online, where widely accessible platforms can be used by criminals to recruit, market, trade, and transact.

At the same time, the development of the online world has effectively helped create new types of crime, such as ransomware attacks on businesses, as well as providing opportunities for criminal activities historically – and thankfully – ghettoized in small criminal networks, such as the distribution of child sexual abuse material (CSAM), to proliferate.

Nor is this period of rapid change over. The increasing adoption of various forms of crypto assets, the development of new, faster payment rails, and, above all, the rise of generative AI suggest that financial crime risks are likely to continue rising. In its 2025 *Financial Crime 360* report, the Payments Association found that 58% of its respondents see AI-enabled financial crime as a "major challenge." Furthermore, 64% were specifically concerned about the potential use of AI to generate synthetic identities, deepfake images, video and audio content that could be used to undermine customer due diligence (CDD) processes, identity and verification (ID&V) and to defraud either their businesses or their clients.

The rapid evolution of these threats has left those on the front lines of defense in a state of heightened alert. Our global survey of 600 senior compliance professionals confirms that these industry-wide concerns are translating into specific, urgent demands for clarity. When asked which areas of underlying crime they would like to see more guidance on, 54% said more information on cybercrime and privacy and 33% wanted more guidance on the Illicit use of decentralized finance (DeFi) to mitigate complex digital risks. While many financial crime risk and compliance professionals are aware of the potential of new technology to enhance the effectiveness of their work, they are also acutely aware that, as 2026 dawns, the conditions for a further boom in technologically enabled crime are rapidly developing.

In supporting your efforts to detect and report organized criminal activity, which areas of underlying crime would you like to see more guidance on?



Source: ComplyAdvantage, The State of Financial Crime 2026

"As we know, criminals are leveraging new AI technologies to create more sophisticated criminal typologies related to fraud, money laundering, and other predicate crimes. While the annual spend on AML technology globally is around $280 billion, we only detect around 0.1 to 0.2% of laundered money. Something has to change."

Andrew Davies
Head of Global FCC Strategy, ComplyAdvantage

Hear more from Andrew in our on-demand webinar: *AI innovation, new regulations, and evolving risks: What's in store for 2026?*

AI: A dual-use technology

One of the most frequent points of discussion among financial crime risk and compliance professionals in 2025 is the impact of AI on the risk and regulatory landscapes. On the one hand, the technological paradigm shift that AI brings has the potential to be a powerful tool for criminals and other malicious actors; on the other hand, it offers the possibility of enhancing the performance of many existing regulatory technology (RegTech) platforms and discovering new ways to identify and mitigate risk. The industry is overwhelmingly committed to this path: our survey found that 99% of organizations report having dedicated projects or budgets specifically for AI solutions in financial crime detection and prevention. Although multiple types of AI exist, four broad categories have made significant progress in recent years:

- **Generative AI** ingests vast amounts of data into large language models (LLMs), which can then produce new text, images, audio, video, and code at high speed.
- **Predictive AI** extrapolates and builds upon existing machine learning technologies to forecast patterns from structured and unstructured data.
- **Agentic AI** understands complex tasks by breaking them down into multiple steps, then learns to apply these steps independently in specific contexts.
- **Robotic AI** encompasses various types of AI models that can be integrated into physical systems to undertake specific practical tasks, either autonomously or semi-autonomously.

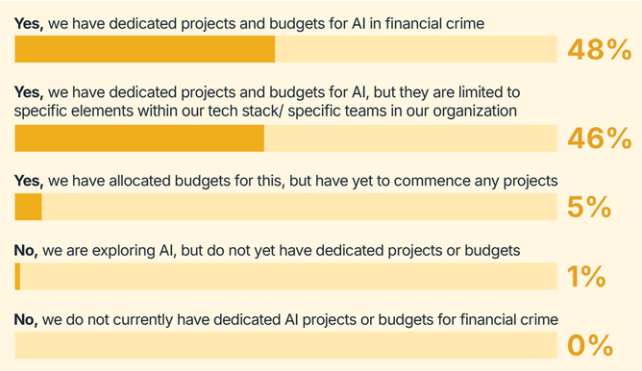
Of these, generative AI (GenAI) has gained the most widespread attention, with growing public use of online LLMs like ChatGPT, developed by OpenAI, and Claude, developed by Anthropic. Governments and businesses have also paid close attention, focusing on the potential for GenAI to drive rapid improvements in productivity and national economic performance: summing up the mood of excitement and expectation, an article in the usually sober journal The Economist asked in July, "What if AI made the world's economic growth explode?"

> *Firms have moved past the question of 'should we use AI?' and are now asking the more sophisticated question: 'How do we use it safely and effectively for the most critical pieces of anti-financial crime work?'*

Iain Armstrong
Executive Director, FCC Strategy, ComplyAdvantage

Hear more from Iain in our on-demand webinar: *AI innovation, new regulations, and evolving risks: What's in store for 2026?*

Does your organization currently have dedicated projects or budgets specifically for implementing or developing AI solutions in financial crime detection and prevention?



Source: ComplyAdvantage, The State of Financial Crime 2026

Nonetheless, as with any new technology, GenAI has raised concerns about its potential for abuse, whether by terrorists, unscrupulous businesses, and, of course, criminals. In recent years, criminal groups, organized and otherwise, have leveraged a variety of new technologies and platforms – mobile phones, instant messaging, social media, end-to-end encryption, dark web marketplaces, 3D printing, and drones, to name a few – to generate illicit profits in everything from the sale of drugs, people, weapons, illegal wildlife and extreme pornography, to the provision of criminal services such as smuggling, the creation of false documentation or access to stolen financial and personal data. It should be of no surprise, therefore, that financial and economic criminals are increasingly exploiting GenAI.

GenAI and financial crime

GenAI has undoubtedly reduced the barriers to entry for financial criminals. Indeed, it is no longer a future risk for the financial services sector, but a clear and present danger. The Financial Action Task Force (FATF) – the international standard-setter on anti-financial crime measures – national regulators, and law enforcement agencies all now see GenAI-enabled crime as a mainstream threat, prompted by a growing number of cases in which LLM-generated material or deepfake-style technology has been used to conceal real identities. Together, they have also expressed particular concern about how LLMs, which can produce material at high speed and in large volumes, are industrializing many elements of financial and economic crime tradecraft. We explore the most notable developments below.

GenAI and fraud

The most visible impact of GenAI has been on cyber-enabled fraud and scams, enhancing 'social engineering' techniques used to convince targets that the perpetrator is someone to trust. UK Finance, a trade association for the banking and financial services sector, reported in autumn 2025 that the recent sharp increase in reported UK fraud cases reflected a growing number of frauds and scams, explicitly linking this to increasingly plausible GenAI-generated material. In 2024, both the FBI and the US Department of Homeland Security (DHS) had already reported that criminals were using LLMs to craft highly tailored emails to trick targets into revealing sensitive information – known as 'phishing' – by using convincing GenAI-generated content in texts, instant messages and emails, translating material into multiple languages for global campaigns, and refining messaging 'on the fly,' effectively A/B testing fraud scripts in real time. GenAI has also been used to optimize fraud volume in other ways. Where sensitive data is already accessible to criminals, either through dark web data markets or undetected business system hacks, LLMS can be used to identify target vulnerabilities and segment them by age, wealth, and other variables, as Europol reports in its 2025 Internet Organised Crime Threat Assessment (IOCTA).

In the investment world, scammers are reportedly using GenAI as well, generating content for 'clone' investment websites that mimic the branding of well-known, regulated businesses or seemingly credible new market entrants, complete with websites, professional-looking collateral, and chatbots that use coherent customer service scripts. This has proven invaluable for those involved in crypto investment scams, where establishing credibility around a new exchange or initial coin offering (ICO) is crucial to success.

LLMs are also playing an increasingly important role in targeting businesses for fraud. One of the most prevalent use cases for GenAI is business email compromise (BEC), where fraudsters deceive senior managers or budget holders into executing payments to criminals or granting access to the firm's business accounts. Here, GenAI can develop more detailed narratives and scripts than in the retail or investment spheres and can generate deceptive audio and video deepfakes. As the Europol Innovation Lab has noted, contemporary CEO fraud (essentially BEC) increasingly employs advanced deepfake technology to deceive busy senior managers and executives. The most emblematic case of recent years in this area has been that of the UK engineering firm Arup, whose staff in Hong Kong were manipulated into sending the equivalent of HKD $25 million to the fraudsters' account in January 2024, using fake audio and video.

Despite the clear escalation of this threat vector, organizations remain highly confident in the effectiveness of legislative response: our survey found that 94% of compliance professionals feel confident that existing and proposed AI regulations in their jurisdiction will effectively mitigate the risk of AI being used to defraud customers (e.g., through deepfakes). However, this high confidence level is viewed with caution by some experts who warn against complacency.

How confident do you feel that the existing and proposed AI regulations in your jurisdiction will effectively mitigate the risk of AI being used to defraud customers in the financial services sector?

Source: ComplyAdvantage, The State of Financial Crime 2026

SHARE THIS

"While it is encouraging that most of the industry feels confident in future AI regulation,

the reality is that the pace of criminal innovation, especially with deepfakes and synthetic identities, will always move faster than legislative bodies.

We cannot afford to wait for the next set of rules to secure our defenses."

Iain Armstrong
Executive Director, FCC Strategy, ComplyAdvantage

Financial institutions are far from immune, either. GenAI has proven to be a powerful new method for generating synthetic identities, new business information, and convincing supporting documentation that can be used to facilitate fraudulent account openings by both retail and business customers; in November 2024, an alert from the US Treasury's Financial Crimes Enforcement Network (FinCEN), the US's financial intelligence unit (FIU), rising numbers of suspicious activity reports (SARs) that noted the use of high quality faked ID and documentation in fraudulent account openings. These accounts can then, of course, be used for a variety of criminal purposes (such as money laundering), but also to undertake loan and credit card fraud against the financial institution holding the account, using more GenAI-generated documentation.

Overall, therefore, GenAI is proving to be an invaluable tool to fraudsters and scammers, increasing the speed and volume at which they can operate, while also massively lowering the barriers to entry in a competitive criminal field.

Click here to see why our mission is to empower every business to eliminate financial crime.

GenAI, extortion, and ransomware

In parallel, GenAI has begun to reshape the practice of extortion. As FinCEN reported in a notice issued in September 2025, '**sextortion**' – the use of faked sexually explicit images, audio, and video to blackmail innocent victims – has boomed in recent years, with teenage boys a particular target in the US. GenAI-generated material has also created opportunities for criminals to develop new styles of extortion, such as '**virtual kidnappings**,' where an individual's voice and image are cloned and sent to unsuspecting families to demonstrate that the individual is in imminent danger, and that a ransom needs to be paid quickly to ensure their safety. Along with fabricating evidence of threat, GenAI can also be used to craft negotiation scripts to manipulate the targets.

The ability to generate convincing fake material and intimidating scripts has obvious implications for ransomware attacks as well. However, one of the most disturbing developments of 2025 has been evidence suggesting that criminals with limited programming skills have now leveraged LLMs to create their own ransomware programmes. In its August 2025 threat assessment report, AI firm Anthropic reported that it had identified a case in which criminals had **exploited its coding-specific model**, Claude Code, in ransomware development. Separately, in the same month, cybersecurity firm ESET reported discovering a new type of ransomware, labeled **PromptLock**, that used GenAI to execute ransomware attacks. Though few, these cases provided further indication of how ingenious criminals are using GenAI to expand their repertoires.

GenAI and money laundering

As noted previously, GenAI can help criminals generate synthetic identities to open accounts for illicit purposes, not least money laundering. One of the standard techniques in laundering is the use of '**money mules**' – individuals who open accounts, deposit and receive funds, and move them on behalf of criminals. In the past, muling has relied on real people – whether witting or otherwise – to both open and/or manage the accounts. However, with GenAI-crafted synthetic identities, backed by convincing ID and social-media backstories, criminals have found ways to create multiple 'virtual' mule accounts (sometimes described as '**account farms**') that can be controlled by a human financial facilitator or even an LLM.

The production of impressive fake business documentation and online 'corporate back stories' is also valuable for launderers who use **corporate and/or offshore vehicles to move illicit funds**. High-end launderers can use LLMs to create stronger paper trails – board minutes, invoices and email chains – that generate an appearance of ordinary, legitimate commercial activity. Similarly, as the FATF has argued, GenAI can be exploited to produce false but internally consistent trade paperwork and develop ingenious mislabelling and goods routing to support **trade-based money laundering** (TBML) and **sanctions evasion** schemes.

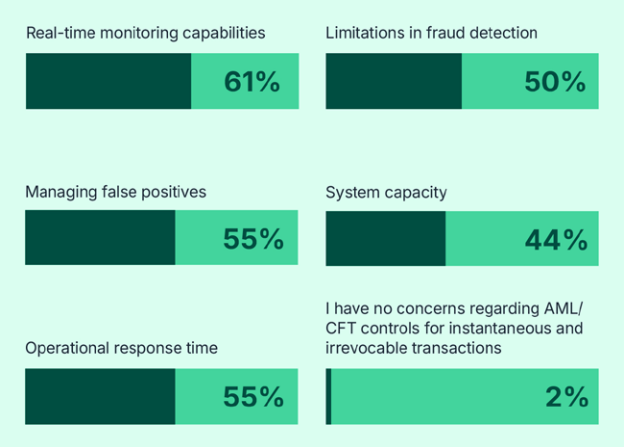
More broadly, GenAI can help criminals in what might be described as 'adaptive' money laundering. LLM-controlled account farms, for example, can be used to probe financial institutions' controls, identifying vulnerabilities in detection systems by experimenting with transaction

patterns, payment references, transaction amounts, and counterparties, to find what works. The net effect of GenAI, therefore, is to improve the scale, scope and speed of money laundering operations, while enhancing their resilience by making fewer mistakes, and adapting faster as businesses change their own controls.

GenAI and the challenge to businesses

The transformation of the financial crime threat landscape by GenAI clearly presents significant new challenges to regulated financial institutions and businesses, the most evident of which is customer identification. If it becomes more difficult to distinguish between real and synthetic customers and clients – especially in an era of remote onboarding and digitized ID&V – firms will face the difficult choice of either onboarding fewer customers, increasing their vulnerability to financial crime and regulatory penalties, or reverting to costly, in-person CDD. The difficulty of verifying these digital identities can create a dangerous ripple effect across the rest of the business. If a fake customer is successfully onboarded, the final opportunity to stop them usually occurs at the point of payment. However, the industry-wide shift toward real-time payments has effectively removed the time delay that once allowed firms to catch these fraudulent transactions before they were finalized.

With the increasing adoption of real-time payments, what are your organization's primary concerns regarding AML/CFT controls for instantaneous and irrevocable transactions?



Source: ComplyAdvantage, The State of Financial Crime 2026

SHARE THIS

When asked about their primary concerns regarding AML/CFT controls for instantaneous and irrevocable transactions,

61% of our respondents cited real-time monitoring capabilities, and 55% were equally concerned about managing false positives and operational response time.

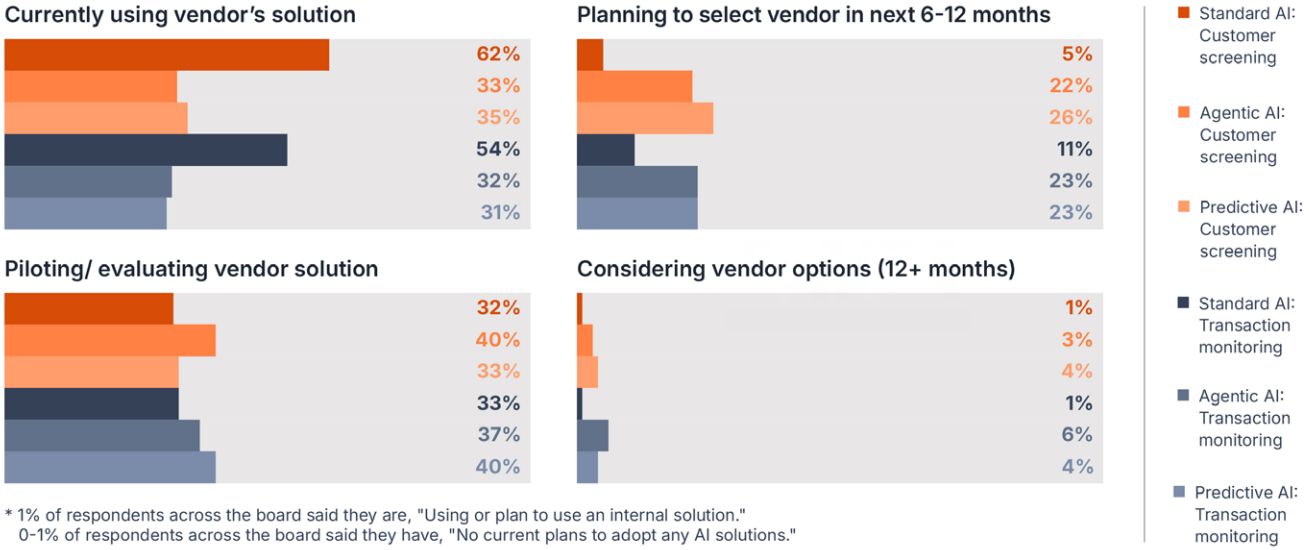
Furthermore, detection systems – for fraud, money laundering, and sanctions evasion – will become progressively more vulnerable. Rule-based transaction monitoring platforms – particularly older, static models – will deteriorate rapidly, generating higher levels of false positives and negatives as legitimate behavior is mistaken for illicit activity, and sophisticated deception patterns escape undetected. AI-assisted obfuscation of names, addresses, and narratives is likely to have the same impact on basic, batch-processed sanctions screening platforms.

Producing actionable suspicious activity reports will also become more challenging, as criminals become increasingly skilled at utilizing LLMs to craft complex yet consistent transactions across multiple institutions and sectors. For FIUs, which are heavily dependent on identifying discrepancies and anomalies between the suspicious activity reports (SARs) of separate institutions, the task of distinguishing the signal from the noise will become even more challenging.

At present, therefore, the weight of the evidence suggests that when it comes to exploiting GenAI, the tactical advantage lies with criminals. Not least, it is a matter of volume and speed: many regulated businesses lack the capacity, capability – even the ability to recognize – the scale and nature of the problem, and risk being drowned as a result.

However, our survey showed the industry is moving quickly to adopt advanced controls: while "standard AI" is already widely used in customer screening (93% of firms currently using, piloting or evaluating), our data shows advanced capabilities are rapidly catching up. The adoption rate for agentic AI in customer screening (73% considering adoption) and predictive AI in transaction monitoring (71% considering adoption) shows the clear shift to more sophisticated, automation-focused solutions. This ambition is validated by expectations: our survey found that 100% of organizations have achieved or expect to see positive outcomes from adopting agentic/ predictive AI. However, current adoption rates for fully implemented solutions lag these high expectations, with only 33% currently using an agentic solution for customer screening and 32% for transaction monitoring.

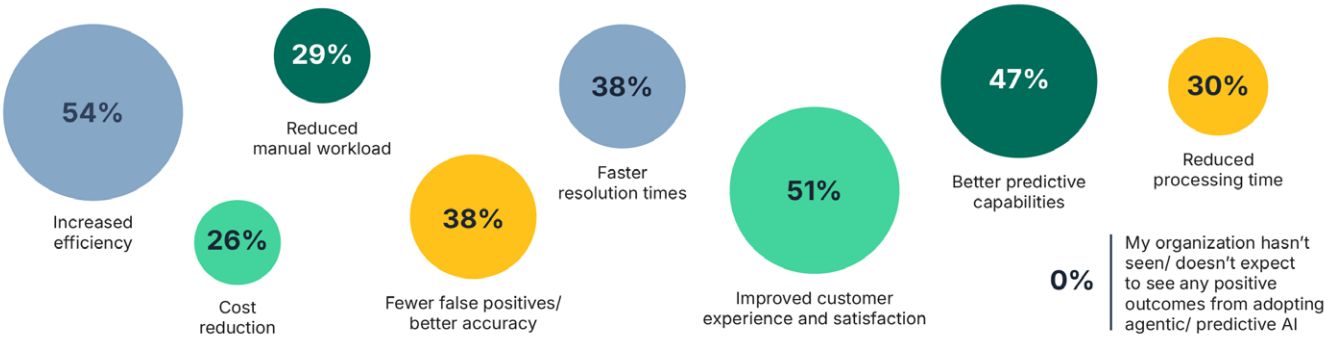
Thinking about AI solutions for customer screening and transaction monitoring, which of the following best describes your organization's stage of adoption?*



* 1% of respondents across the board said they are, "Using or plan to use an internal solution."
0-1% of respondents across the board said they have, "No current plans to adopt any AI solutions."

Source: ComplyAdvantage, The State of Financial Crime 2026

What positive outcomes has your organization achieved/would expect to see from adopting agentic/predictive AI?



Source: ComplyAdvantage, The State of Financial Crime 2026

Glossary

For the purpose of our survey, the term **'agentic AI'** describes AI models that are equipped with agency: the ability to plan, reason, and execute tasks in pursuit of objectives. Unlike **'standard AI'** systems that are limited to a single output (eg. a model that flags a transaction as suspicious based on a pre-set rule), agentic AI can interact with external tools, adapt behavior based on context, and operate iteratively until the desired outcome is achieved. An example of agentic AI is the auto-remediation of level 1 alerts – where the AI not only identifies a low-risk alert but also independently gathers the necessary data, drafts the closure narrative, and closes the case without human intervention.

Predictive AI forecasts future outcomes by analyzing data patterns, while agentic AI acts autonomously to achieve goals by combining predictive capabilities with autonomous planning, decision-making, and action-taking in an environment, often involving multiple agents working together with human guidance or oversight. The key difference is prediction (what might happen) versus autonomous action (making it happen).

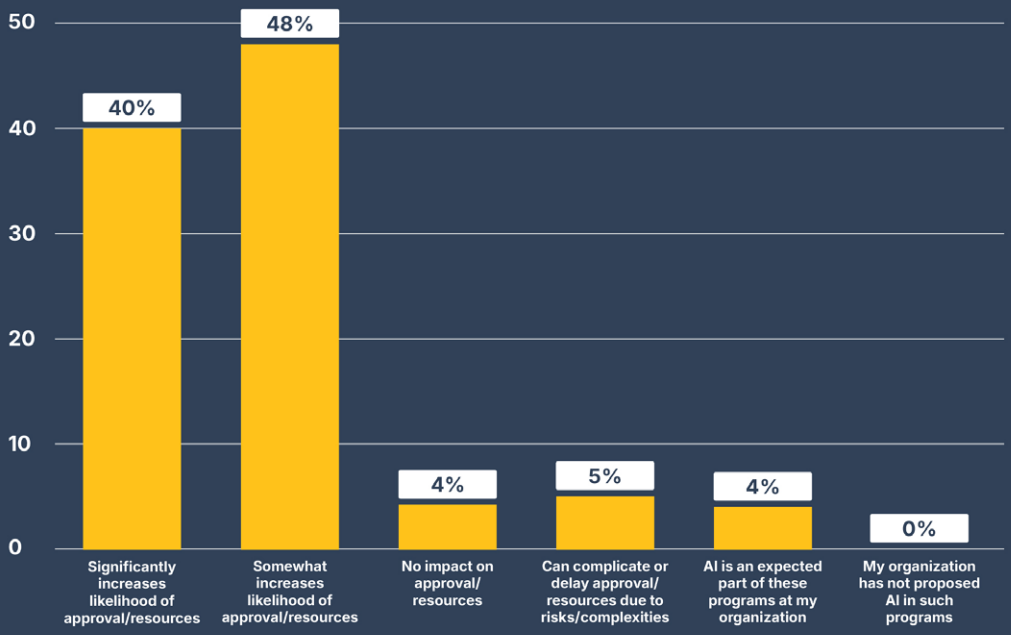
If we are going to implement AI and agentic solutions, we must establish the necessary documentation and governance on the back end. You must be really prescriptive in terms of what the desired outcomes are and how we QA it; because if you go into any regulatory exam or inquiry without that paper trail, you leave your organization completely exposed to the highest level of scrutiny. You need to make sure you dot your I's and cross your T's and document everything.

Nick Passarelli
Chief Compliance Officer,
Melio

Read more about Nick's perspective on today's modernized approaches for enhanced risk management here.

And this does not even consider the issue of quality. As GenAI develops, LLMs will produce more convincing synthetic identities, more impressive business documentation, and more complex fraud and money laundering typologies. Add to this the development of agentic AI, which will act, learn, and react with growing autonomy, as well as predictive AI, which probabilistically models the most effective typology; the prospect for regulated businesses is daunting. Nor is this science fiction: the World Economic Forum (WEF), the UK's National Cyber Security Centre (NCSC), and Europol, the combination of different elements within a growing AI stack, will provide criminals and other bad actors with the capability to automate complex, rapid attack chains across a variety of domains, including financial crime. Nor will this be a static problem, as criminals rapidly seek to optimize performance, unencumbered, as businesses will be, by constraints such as organizational structures, costs, governance, and regulations. However, the industry is highly motivated to overcome these challenges, recognizing that AI adoption is necessary to keep pace with the accelerating 'AI arms race' in financial crime. When asked about the impact of including AI in a compliance modernization program, 88% of organizations reported that it significantly or somewhat increases the likelihood of gaining approval and securing resources.

What impact does including AI in a proposed financial crime compliance modernization program have on the likelihood of gaining approval and securing resources?



Source: ComplyAdvantage, The State of Financial Crime 2026

What does this mean for my firm?

The picture is not totally one-sided. Regulated businesses are also deploying various types of AI across their technology stacks to 'fight fire with fire.' The positive outcomes, according to our survey of advanced AI users, are clear: 54% of organizations report increased efficiency, 51% cite improved customer experience, and 47% note better predictive capabilities. Common use cases include:

- **CDD/KYC:** Firms are utilizing LLMs to review CDD/KYC packs, reconcile data against registries, and generate risk profiles for human review. In fact, 41% of organizations currently using, piloting or evaluating advanced AI solutions have implemented automated customer onboarding/KYC processes. Beyond initial checks, agentic AI enables **perpetual KYC** by detecting real-time behavioral shifts. LLMs also handle the "heavy lifting" in periodic reviews by flagging only significant inconsistencies since the last check.
- **IDV and payments:** To counter deepfakes, firms are adopting "liveness" analytics – AI tools that detect synthetic artifacts in images and audio. Additionally, GenAI-powered chatbots now insert contextual questions into authentication processes to identify fraudulent or synthetic behavior.
- **Fraud detection, transaction monitoring, and screening:** AI adoption is accelerating across monitoring platforms, with 55% of organizations reporting improved suspicious activity detection, 53% reporting enhanced transaction monitoring, and 38% reporting enhanced risk scoring. Multiple analyses, including research from the **Bank of England**, suggest that AI-driven pattern detection, when appropriately governed, can dramatically reduce false positives. GenAI has demonstrated value in helping design and refine detection rules, as well as creating realistic synthetic data for system testing. Predictive AI is also being used to supplement rules-based detection with baseline customer behavior modelling, flagging subtle deviations in customer behavior that would not otherwise be detected. Importantly, predictive AI is also being used to stress-test institutions' own controls, identifying unknown vulnerabilities and testing system performance against emerging typologies.
- **Triage, investigations, and reporting:** AI acts as a "force multiplier" for compliance professionals overwhelmed by the volume of alerts. LLM-powered "co-pilots" cluster hits and collate data into investigation packs, while GenAI drafts narratives for SARs. Quantifiable progress is being made across these high-volume workloads: 40% of organizations have implemented streamlined case investigation, 39% have implemented automated regulatory reporting, and 32% have implemented auto-remediation of Level 1 alerts.

In 2026, firms face a unique paradox: AI is simultaneously the primary enabler of financial crime and the most vital tool for its control. While the balance currently favors criminals, firms can tilt the scale back by embedding AI quickly and safely. Success depends on whether regulated institutions can outpace attackers who are already utilizing these technologies at scale.

Andrew Davies
Head of Global FCC Strategy, ComplyAdvantage

Crypto and the currency of crime

AI was not the only technology gaining widespread attention in the financial crime world in 2025. By the end of 2025, crypto assets – now well over a decade old – were becoming firmly established and integrated into the global financial ecosystem. In October, the IMF reported that crypto's total market capitalization stood at around $4.2 trillion, and that the market value of stablecoins – virtual assets pegged to a fiat currency, a commodity, or a stabilizing algorithm – had exceeded $300 billion. Naturally, the same features that made crypto appealing to investors – liquidity, transactional speed, relative if not total anonymity – have also rendered it highly attractive to criminals. The blockchain analytics firm Chainalysis estimated in its 2025 mid-year report that over $2.17 billion in cryptocurrency had already been stolen year to date. Among crypto asset service providers, decentralized finance (DeFi) – financial applications allowing financial transactions on a public blockchain without traditional intermediaries – remained a popular target for crypto hackers. So too, however, did centralized cryptocurrency exchanges, with compromised private keys proving one of the most significant vulnerabilities.

> *I think a lot of crypto businesses, and especially a lot of stablecoin issuers, have started to see that being [...] well-regulated and highly compliant is a huge competitive advantage. And I think that's how you really future-proof your business, your team, for the adoption of stablecoins at an institutional and broader level.*

Angela Ang
Head of Policy and Strategic Partnerships, APAC, TRM Labs

Hear more from Angela in our on-demand webinar: *New rules, new risks: Navigating stablecoin compliance in APAC*

This was not to suggest, of course, that crypto was solely or even mainly used for criminal purposes. As annual reports from blockchain analytics firms such as Chainalysis and TRM Labs regularly show, less than 1% of all crypto transaction volumes are linked to illicit transactions in any given year. Although this is partly reassuring, it's important to remember that although most fiat transactions are not illicit either, illegal activity involving fiat is clearly of concern. Crypto does not get a pass, any more than fiat. What is more, it is becoming obvious how widely criminals are adopting crypto across a range of different crime types.

Crypto does not get a pass, any more than fiat. What's more, it is becoming obvious how widely criminals are adopting crypto across a range of different crime types.

Fraud and scams

As noted in the previous section on AI, these crimes based on deception or threat have been turbo-charged by the arrival of the internet and further enhanced by more recent technological developments. Based on recent cases and studies, the prominence of crypto as criminals' currency of choice is evident, especially in the 'pig-butchering' scams associated with scam centers in Southeast Asia (see Chapter 2: Geopolitics and sanctions). Here, victims are tricked into investing larger amounts over time – sometimes lured by romantic blandishments, or the promise of incredible returns, among other incentives. In these cases, scammers insist that their victims invest in crypto assets. According to an investigation by blockchain analytics firm Elliptic, Huione Guarantee, an escrow marketplace within the Cambodian Huione Group, has played a significant role in collecting proceeds from pig-butchering scams, collecting around $89 billion in crypto, much of it in the stablecoin Tether. In October 2025, the US also indicted Chen Zhi, founder of the Prince Holding Group, another alleged industrial-scale pig-butchering operation in Cambodia. As part of a joint action with the UK, the US seized around $15 billion in Bitcoin. While in both cases not all the funds have been definitively linked to pig butchering or other frauds, both Huione and Prince groups have been accused of enabling other criminal activities – the apparent nexus with so much crypto remains striking.

Ransomware and extortion

Ransomware and extortion operations also overwhelmingly favor crypto as a payment method, with fiat-based approaches increasingly dying out. Most ransomware operators continue to demand payment in Bitcoin, but privacy coins, which obscure transaction details through encryption, such as Monero, have become more popular in recent years. Chainalysis found that 2024 was the highest-grossing year for ransomware payments, with ransomware groups increasingly choosing fewer, larger institutional targets (known as 'whale' or 'big game' hunting). The year also saw one of the largest ransomware payments ever recorded: $75 million to the 'Dark Angels' ransomware group. 2025 reporting also suggested a growing number of ransomware attacks. However, as cybersecurity firm Deep Strike found in November, the amounts being paid were falling, apparently due to victims' growing unwillingness to pay.

Hacks and thefts

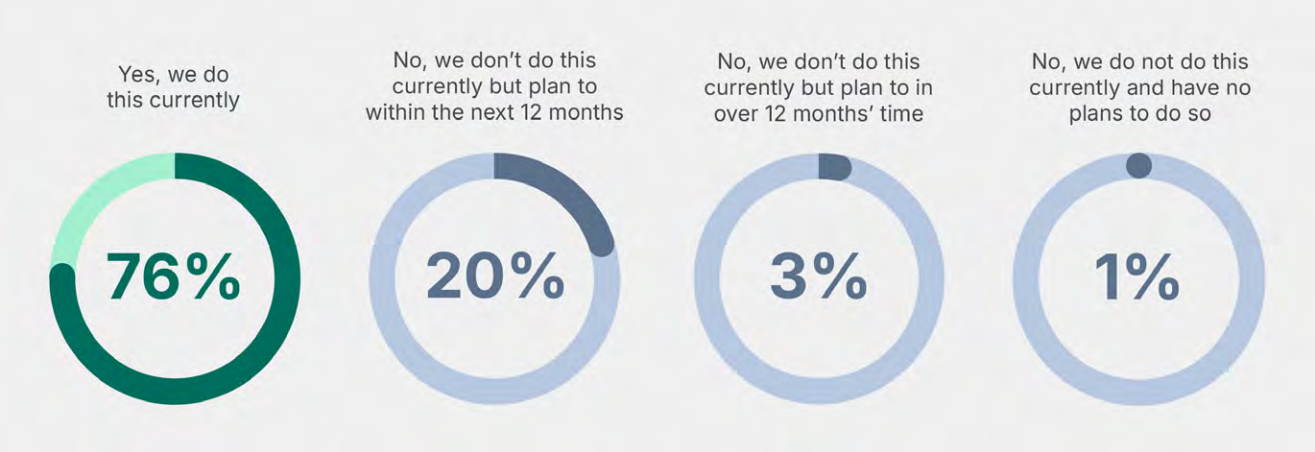
As noted earlier in this section, the scale of direct cryptocurrency theft has increased over recent years, with 2025 proving to be one of the most significant on record. Mid-year, Chainalysis predicted that by year-end, the then-current cumulative amount of stolen crypto – $2.17 billion – could rise to more than $4.3 billion.
The most notable heist of the year was the attack by the North Korean state actor 'the Lazarus Group' on crypto exchange Bybit in February, which resulted in the theft of crypto worth around $1.5 billion from a 'cold wallet,' held offline, and thus supposedly more secure. It is believed to be the largest single hack in crypto history, accounting for most of that amount. However, the year also saw an increasing number of smaller attacks on DeFi services and 'wrench' attacks against personal wallets.

Illicit markets

Crypto now significantly underpins 'traditional' organized crime, becoming the preferred payment method in various online dark net illicit markets and covertly through fake e-commerce sites, social media, and encrypted messaging platforms. A 2025 report by the think tank the Global Initiative against Transnational Organized Crime (GI-TOC) argued that a "digital drug revolution" had transformed the way illegal narcotics and illicit prescription drugs are sold, enabling illicit drugs to reach new markets such as rural areas of Scotland and the US Midwest, while also encouraging consumers to buy in bulk and explore a wider variety of drugs. In most cases, customers are required to purchase illegal drugs using cryptocurrency. Quoting figures from TRM Labs, the think tank stated that over $1.7 billion in crypto-denominated drug sales occurred in 2024, marking a more than 20% year-on-year rise. Other core organized crimes have been affected too, including weapons trafficking, human trafficking and modern slavery, illegal migration, and even wildlife crime, where criminals are looking to take payments for the delivery of illicit payments and services in Bitcoin, Tether, and privacy coins such as Monero. Although the volume of products in some of these markets bought with crypto probably remains a relatively small proportion of the overall amount – illicit drug dealing still relies heavily on cash – the long-term trend is undeniably towards a greater use of crypto as a currency of choice.

The widespread nature of organized crime activity utilizing cryptocurrencies highlights the critical need for formalized risk assessment frameworks. When asked, "Does your organization include a detailed analysis of its exposure to organized crime activities in its organization-wide risk assessment?", 76% of organizations confirmed they currently do this. This demonstrates strong, though not universal, commitment to assessing high-impact threats. However, the challenge of strategic oversight remains: 24% of organizations are not currently including a detailed analysis of organized crime exposure, although 20% plan to do so within the next 12 months. This means that, despite the massive scale of illicit activity being reported, a significant minority of firms lack a formalized process to quantify and mitigate their exposure to the very activities that generate the most money laundering risk.

Does your organization include a detailed analysis of its exposure to organized crime activities in its organization-wide risk assessment?



Source: ComplyAdvantage, The State of Financial Crime 2026

Money laundering

Blockchain analytics firms now view money laundering – broadly defined – as the main use case for illicit cryptocurrency. Chainalysis's 2025 Crypto Crime Report and mid-year update reveal that most illegal transactions stem from scams, hacks, darknet markets, and ransomware, rather than from the initial 'predicate' transactions themselves. TRM Labs research shows, for example, that Latin American cartels have extensively integrated cryptocurrency into their money laundering operations for both cross-border settlements and layering, including in their dealings with Chinese money laundering organizations (CMLOs) (see pages 32-41). The methods used to launder crypto are also becoming more advanced. While crypto tumbling and mixing services have attracted increasing regulatory and law enforcement attention, recent reports suggest that 'chain hopping' – quickly transferring value across different blockchains, often via unregulated bridges and instant coin-swap services – has become the preferred method for launderers to avoid detection. Stablecoins – especially Tether – have also recently gained popularity for laundering, mainly because they are less volatile and less stigmatized than a 'pure' cryptocurrency such as Bitcoin. As the crypto ecosystem grows and becomes more intricate, it appears that money launderers have made it a key element in their repertoire.

The rising frequency and technical sophistication of these blended attacks – which involve both cyber intrusion and subsequent money laundering – highlights the failure of siloed financial crime defenses.

> *Historically the AML and fraud risk management functions in many financial institutions did not share the same reporting line, resulting in the pursuit of different strategies and tools. But today we more often see those functions coming together to align on their data and tech opportunities and solutions.*

Mike Bowman
Financial Crime Advisory
Kroll

Read more about Mike's perspective on today's modernized approaches for enhanced risk management here.

Terrorist financing

The consensus among experts is that crypto assets have become an operationally valuable component in terrorist financing. In its 2025 Comprehensive Update on Terrorist Financing Risks, the FATF highlights the increasing use of crypto assets by ISIL affiliates like ISKP in Afghanistan, Al-Qaeda-linked groups, and Hamas in Palestine. Here, crypto's primary role is raising funds through 'pop-up' crowdfunding campaigns on social media and instant messaging platforms, where fundraisers share QR codes and/or wallet addresses for donations, often requested in privacy coins or stablecoins. Crypto transfers are also used to send cross-border funds among facilitators in different regions. Nevertheless, this remains only a supplement to the existing terrorist financing toolkit, which – especially for Islamist extremists – still relies heavily on a combination of cash couriering, wire transfers, bank transactions, TBML, and informal value-transfer systems like Hawala to move funds internationally.

Sanctions evasion

The topic of sanctions evasion is thoroughly examined in our 'Geopolitics and sanctions' chapter; however, it is also essential to highlight the growing role of crypto in this section. Blockchain analytics firms generally agree that activities related to sanctions form the largest share of known illicit crypto use. In its 2025 report, Chainalysis estimated that sanctioned jurisdictions and entities received approximately $15.8 billion in cryptocurrency in 2024 – about 39% of the total illicit crypto transaction volume.

Similarly, TRM Labs' 2025 report found that sanctions evasion made up roughly one-third of illicit crypto transactions in 2024, surpassing fraud and darknet markets. North Korea remains, of course, the most notable example of a state using crypto to bypass sanctions, replenishing the regime's funds through the value generated from cyber thefts – converted into fiat – to support its illegal weapons proliferation activities. However, crypto also plays a role, to varying degrees, in the strategies of other countries. For example, in June 2025, the US Department of Justice indicted Russian national Iurii Gugnin for allegedly running a large-scale sanctions-evasion network that accepted payments from Russian clients in Tether, then routed the funds through multiple exchanges before purchasing sanctioned luxury goods and sensitive technology.

It is, of course, important to emphasize that despite North Korea's pioneering efforts, crypto has not replaced traditional methods of buying and selling sanctioned goods, especially for hydrocarbon-rich nations like Russia and Iran. Trade-based schemes involving front companies, the conventional banking system, and, in Iran's case, Hawala, still dominate. Nonetheless, crypto has developed alongside these methods as an additional layer of obfuscation, exploiting gaps between jurisdictions and between traditional and crypto asset supervision.

What does this mean for my firm?

Crypto now permeates every aspect of the AML/CFT landscape; it is no longer a niche but an integral part of mainstream financial infrastructure. It is also deeply intertwined with the modern illicit economy: The practical implication for regulated firms is clear: crypto cannot be treated as something 'separate.' Consideration of crypto risk must be integrated into existing governance and control frameworks, while respecting its unique technical features and current risk profile. Regulated firms thus need to consider several issues:

- **Governance:** CASPs need a dedicated crypto risk assessment that details the specific risk exposures of their products, channels, and customers. The FATF's **risk-based approach** remains the standard: board-level oversight, appointed and named leadership, and regular reassessment of risks as technologies evolve. However, other financial institutions with direct and indirect exposure to the crypto ecosystem must also consider the risks entailed and respond accordingly.
- **Licensing, CDD, and KYC:** Any firm offering crypto services must be appropriately licensed in its home jurisdiction, and those dealing with CASPs must verify that their counterparties are authorized. When onboarding or managing crypto-intensive businesses, firms must now apply enhanced due diligence as a standard; this includes understanding their business model, customer base, and international footprint, as well as their reliance on riskier services like DeFi or over-the-counter (OTC) brokers.
- **Travel Rule and counterparty risk management:** Getting this right is non-negotiable. Collecting, holding, and transmitting originator and beneficiary information for qualifying crypto asset transfers is a basic expectation. Effective implementation now requires Travel Rule-compliant messaging with major CASPs, supported by RegTech where available, and structured counterparty risk assessments. Such a rigorous approach is not only good compliance but also good risk hygiene: understanding which counterparties are safe to deal with and which should be avoided or exited.
- **On-chain monitoring and analysis:** For those offering crypto-asset services, on-chain monitoring should be fully integrated into firms' transaction monitoring suites. Screening deposits and withdrawals against addresses linked to sanctions, ransomware groups, darknet markets, scam networks, or wallets frozen by stablecoin issuers is now both practical and standard practice. Similarly, monitoring transactions involving suspect mixers and high-risk crypto exchanges is crucial for firms to identify attempts at customer obfuscation.
- **Cybersecurity:** **The FATF's 2025 update** on CASP risk management emphasizes that cyber intrusions into financial service providers are both financial crime and cybersecurity risks. CASPs should therefore strengthen their infrastructure and security protocols and continuously review them, given the constantly evolving hacking techniques and methods.
- **Public–private cooperation:** Public–private partnerships like the UK's **Joint Money Laundering Intelligence Taskforce** (JMLIT) now have a strong track record of providing insights into emerging criminal typologies and threats. Unsurprisingly, the FATF explicitly encourages crypto-native businesses to participate in such collaborations and to use law enforcement intelligence to enhance their transaction monitoring, investigations, and suspicious activity reporting.

The overall message for regulated firms should be that crypto assets are neither unusual nor marginal. CASPs clearly need to operate carefully to manage risks and adhere to financial crime standards, but other firms with exposure should also consider how they adapt their AML/CFT systems to meet the challenge. Those that do – supported by appropriate analytics, governance, and controls – will be best positioned to manage the risks now at the intersection of fiat and blockchain finance.

Iain Armstrong
Executive Director, FCC Strategy, ComplyAdvantage

The predicate offence: Cyber fraud

Fraud, especially cyber fraud, has been discussed in our previous sections on AI and cryptocurrency. However, it requires more focused attention: fraud, after all, now plays a central role in the global crime economy. Measures vary between jurisdictions, and no comprehensive global estimate exists, but the trend is evident. UK Finance, for instance, informed Reuters that 3.31 million fraud cases were recorded in 2024, resulting in losses of £1.17 billion. The UK's National Crime Agency (NCA) also reported that fraud accounts for 41% of all recorded crime in the country.

Cyber fraud and cyber-enabled fraud are becoming increasingly dominant in this fraud landscape. The FBI's 2024 Internet Crime Report, released in April 2025, recorded 859,532 complaints and more than USD 16 billion in reported losses from cyber-enabled crimes, including fraud and scams. UK figures reinforced this picture. The UK Economic Crime Survey for 2024, published in November 2025, found that around 40% of business frauds had been facilitated by cyber means, usually through email phishing. The UK's Crown Prosecution Service's (CPS) 2025 review suggests an even more striking picture: fraud has become "cyber-enabled, serious and organised," with an estimated 80% of reported cases involving some cyber element. Cyber-enabled fraud is also a major industry. Research published by the UN Office on Drugs and Crime (UNODC) in April 2025 indicated that scam centers in Southeast Asia generated almost $40 billion annually. It further suggested that model has begun spreading to Africa, Latin America, and the Middle East. Law enforcement activity also reflects its growing prevalence: in November 2025, INTERPOL, the international law enforcement agency, announced the completion of a 40-country operation, HAECHI VI, with disrupting cyber-enabled fraud and scams as a key goal.

Cyber frauds against individuals

Modern cyber-enabled frauds and scams targeting individuals generally fall into a small number of well-known categories, each adapted by digital technology, instant payments, and, as noted previously, GenAI. Phishing and social engineering act as the primary entry methods. Authorized push payment (APP) schemes use manipulation to enable quick bank transfers. E-commerce and card-not-present fraud exploit the shift to online shopping. Identity theft and account takeovers are driven by large-scale data theft behind the scenes. Investment scams, such as 'pig-butchering,' as well as romance scams, are the highest-value long-term schemes, often operated by scam centers that target victims worldwide.

Phishing

Most victims initially encounter fraud through an email, text message, or an unexpected call pretending to be from the police or a bank. A request to follow a hyperlink or grant remote access then follows, leading to direct account theft or pressure to transfer funds. The FBI has highlighted phishing as one of the major scams facing the US in 2025, particularly targeting older Americans. Europol's 2025 IOCTA also emphasized phishing as a key issue, noting that it remains the most common cyberattack in Europe, used to steal credentials, deploy malware, and hijack accounts. Emerging tactics include malicious QR codes – called 'quishing' – hidden in emails, posters, or websites, and AI chatbots that mimic customer service or banking representatives, guiding victims through 'security checks' and convincing them to share one-time passwords or card details.

The quantitative data show inconsistency but remain informative. Australia's National Anti-Scam Centre recorded 52,753 phishing reports to Scamwatch in 2025, which is a decrease from 80,119 in 2024, along with a 47% decrease in remote-access scam reports; however, it still highlights that phishing scams continue to disproportionately affect older Australians, who lose more and find it more challenging to recover from these scams.

Authorized push payment fraud

Authorized push payment (APP) fraud occurs when individuals mistakenly believe they are making a payment to a trusted counterparty, such as their bank, a government agency, a business, or even a family member or friend, and willingly proceed with the transfer. To all intents and purposes, the payment seems legitimate. By the time the transfer reaches the receiving account, it is considered 'authorized' and often appears indistinguishable from any other payment. UK Finance's 2025 Fraud Report stated that there were £450.7 million in UK APP losses in 2024, of which £365.7 million were consumer-specific. Although the number of APP cases had dropped by approximately 20% year-on-year, they still represented a significant proportion of individual losses. Data from UK Finance for the first half of 2025 also showed £629 million in fraud losses, of which £257.5 million came from APP fraud – two-thirds of which were initiated online, and 16% via phone. This marked an 8% decline in the number of cases from the same period in 2024, but a 12% rise in losses. Although the UK is among the few jurisdictions to produce consolidated figures on the prevalence of APP fraud, reporting suggests it is also causing significant and growing problems in major markets across the Americas and Asia.

E-commerce frauds

An increase in online consumer spending over the last decade has driven a rise in e-commerce fraud and card-not-present (CNP) abuse. For individuals, this includes spending money with fake online stores and non-delivery scams on marketplaces and social media, or the abuse of consumer card details, often facilitated by criminal data breaches or card cloning. UK Finance's 2025 Fraud Report found that an overall trend downwards in unauthorized card fraud had reversed in 2024, with a 22% rise in cases driven mainly by an increase in remote purchase fraud, where card-not-present transactions were made over the internet or phone. In Australia, too, the ACCC has noted a surge in online 'shopping scams' via fake websites, social media ads, and marketplace listings, with Australians reporting nearly AUD 260 million in losses in the first nine months of 2025.

Identity fraud and account takeover

Phishing, APP, and various forms of e-commerce fraud often originate from identity theft. Europol's IOCTA 2025 identifies identity theft as a major driver of modern cyber fraud, facilitated by access to breached or stolen account details and card credentials purchased in bulk on dark web markets. Using this data, fraudsters can access existing accounts – account takeover – or use stolen credentials to open new accounts and obtain credit. Victims may remain unaware until they notice unexplained credit applications, charges for loans they never asked for, or when they check their credit records. Once again, global data on the prevalence of ID theft and account takeovers are hard to find. However, figures from Cifas, the UK's not-for-profit fraud prevention organization, indicate it to be a widespread phenomenon, noting that in 2025 most frauds (around 60%) reported to its National Fraud Database (NFD) involved identity theft, with 249,417 cases recorded in 2024 – a 5% increase from the previous year.

Investment fraud and 'pig-butchering'

The most remunerative frauds targeting individuals in Western and Asian markets are now investment and 'pig-butchering' scams. Operationally, as noted previously, these scams rely heavily on crypto and fake platforms and have become more effective in recent years with the development of GenAI. These long-term scams can run over weeks or months, usually via messaging apps and social media. Initial contact is framed as friendship or romance; only later does it morph into trading tips, access to an 'exclusive' fund, or guidance on crypto and FX trading. Victims are persuaded to move funds that mimic legitimate trading environments but are in fact controlled by criminals. The proceeds are then funneled through crypto exchanges and various mule accounts, often crossing borders several times. The combination of emotional grooming and apparently sophisticated financial products makes such scams unusually hard to tackle; victims frequently do not see themselves as victims until it is too late, by which time, their funds have long since left the country.

As the UNODC states, most of these scams currently emanate from 'scam centers' in Myanmar, Cambodia, Laos and neighboring areas, where trafficked workers are forced to execute the frauds against victims in North America, Europe, East Asia and Australasia. These compounds – heavily linked to forced labor and human trafficking – run thousands of simultaneous scams (romance, investment, crypto plays, fake job offers, etc.) using scripts, customer relationship management (CRM) platforms and multilingual content. The global scale of investment scams and pig butchering worldwide is unknown, but most assessments suggest they are large and growing. As Chainalysis reported in February 2025, they generated the two largest crypto scam hauls in 2024, taking 50.2% (investment) and 33.2% (pig-butchering), respectively. National data, when available, also provides some indication of the impact of these scams. The FBI reported in April 2025 that investment fraud formed the largest single category of loss for victims in 2024. In Singapore, Police Force data for the first half of 2025 show investment scams as the leading type by monetary loss, accounting for 31.9% of the total.

Romance scams and sextortion

Romance scams often overlap with investment fraud, blending elements of love, financial deception, and sometimes sexual blackmail. These schemes frequently involve using deepfake or stolen intimate images (a variant known as 'catfishing') to build a relationship online, build trust and empathy, before seeking financial support through cryptocurrencies, mobile payment apps, gift cards, or bank transfers, or coercing the payments by threatening to 'doxx' victims by sharing intimate pictures of them with family or employers. Most reports indicate that these scams originate from Southeast Asia, as well as from Eastern Europe, the Middle East, and West Africa. INTERPOL's 2025 operations targeting the African aspect of the issue have revealed sophisticated schemes utilising multiple channels – dating apps, social media, and instant messaging – to lure and coerce victims through sexual manipulation.

Until recently, many experts believed this crime was under-reported due to victim shame,

but increased media coverage might now be reducing the stigma. National data emphasizes their significance. Australia's Targeting Scams 2024 report shows that romance scams are the country's second-largest type of scam by loss volume (AUD 156.8 million) after investment scams. In October 2025, the UK financial regulator, the Financial Conduct Authority (FCA), also issued a statement describing romance fraud as a "growing financial crime," with case numbers rising by 9% over the previous year. Financial institutions need to do more to support victims, it stated, noting that often, the emotional impact of the crime was more challenging for victims than the financial loss.

Cyber frauds against businesses

In advanced economies, cyber-enabled fraud has become the primary type of financially motivated cybercrime affecting businesses of all sizes – from SMEs to large firms. Although methods vary across sectors, the main drivers remain the same: digital communication, stolen credentials, and rapid payments, with an increasing role for GenAI.

Business email compromise (BEC) and its variations are arguably the most well-known categories of cyber-enabled corporate fraud. They have much in common with APP fraud – the difference being that the funds involved are much larger. The typical scenario involves fraudsters using compromised or spoofed corporate email accounts or other corporate communication channels to deceive those with authority over company finances into making urgent payments, changing a major supplier's banking details, or granting access to company finances, using a powerful pretext (known as 'pretexting'). These kinds of payment diversion techniques are a particularly acute problem in sectors with complex supply chains such as construction, professional services and manufacturing, where high-value invoices and payments are routine.

As mentioned earlier, this type of fraud has been enhanced by GenAI techniques (see, for example, the previously mentioned Arup case). In the US, the FBI's latest figures indicate that BEC is the second-largest category of fraud losses (after investment fraud), totalling around $2.8 billion. Europol's SOCTA 2025 also describes BEC as one of the "most prolific" online fraud types, alongside investment scams. In the UK, the government's Economic Crime Survey does not specifically include a category for BEC; however, its 2024 report found that 27% of surveyed businesses had experienced 'mandate fraud' (attempts to persuade a company to alter payment details for a supplier), making it the second most common form of business fraud experienced in the UK.

BEC is not the only type of fraud businesses face, however. Other standard and widely experienced categories include:

- **First party frauds:** The term 'First-party fraud' is often used interchangeably with others, such as 'friendly fraud' and 'chargeback fraud.' In essence, they all describe a situation in which a customer disputes a transaction – often made online with a card – to get a refund while keeping the product or service. While there are very few official statistics on these types of fraud, industry surveys and anecdotal reports from card providers and trade associations suggest that the problem is widespread and on the rise. For businesses – especially those operating mainly or solely online – 'losses' also extend beyond the transaction itself to reputational harm and a potentially higher fraud risk classification with financial services providers.
- **Insider frauds:** Firms face a variety of insider fraud risks facilitated by cyber manipulation of internal processes, such as salary, expenses and supplier payments, which are used to divert funds. Common examples include fake emails from senior managers or Human Resources to financial teams requesting changes to payment amounts or details, interference with payment systems, or the manipulation of expense claims.
- **First-party/insider frauds:** A final category worth noting is collusive fraud involving both outside actors and business insiders. In May 2025, the Association of Certified Anti-Money Laundering Specialists (ACAMS), a professional association, working with Cifas, highlighted this as a growing threat area, citing examples such as the deployment of remote IT workers into Western firms by North Korea and the case of Jan Marsalek, the former Chief Operating Officer (COO) of German FinTech Wirecard, who fled to Russia in June 2020 after a hole equivalent to around $2.1 billion was found in the company's accounts. Marsalek was subsequently revealed to be a Russian intelligence asset.

Overall, these patterns show how cyber-enabled fraud against businesses has become a complex threat that exploits both technological and organizational vulnerabilities. The key enablers – such as compromised digital identities, real-time payment systems, and advanced social-engineering methods – are common across external, internal, and collusive forms.

Finally, it is crucial to recognize that cyber fraud poses a significant issue for a specific part of the private sector: financial services. Cyber fraud challenges the industry in several notable ways. Most obviously, there are the direct monetary losses caused to customers and, where credit is extended, to the financial institution. Additionally, there are the indirect costs of identifying, investigating, and resolving the fraud, as well as lost business if a customer decides to switch to another provider because of the incident. In some jurisdictions, there is also the issue of who bears the loss; several countries have voluntary – and in one case mandatory (the UK) – reimbursement schemes that, under certain conditions, make the financial services provider responsible, to varying degrees, for refunding the customer's losses. An even more insidious long-term damage is reputational. Falling victim to fraud can significantly diminish customer trust in their financial services provider. If the scale or scope of the fraud becomes widely known, it can deter new customers, influence market sentiment, and lead to increased scrutiny and criticism from regulators, as seen in Australia. An explosion of fraud at a financial institution can indicate a failure of due care towards customer needs and may suggest management negligence in the face of criminal exploitation. While much media attention has focused on how banks handle fraud, the sector most at risk are undoubtedly FinTechs. Relying on digital architecture and lacking the deeper financial reserves, long-term reputations, and regulatory relationships of traditional banks, they are highly vulnerable to the full range of risks that cyber fraud presents.

Cyber fraud trends

The modern cyber fraud environment displays several key traits.

- Firstly, there is the increasing role of technology: the internet, social media, mobile devices, GenAI, and crypto have all greatly enhanced fraudsters' ability to target numerous potential victims, whether directly or through stolen data, quickly establish the trust or access needed to carry out financial transfers, and move funds securely via fast payment networks before dispersing them through various channels. The cyber fraud economy might thus be well described by the title of the old car heist film *Gone in 60 Seconds*, except that 60 seconds is an eternity in cyber fraud today.
- A second important characteristic, naturally following from the first, is industrialization, as shown by the widespread scam hubs that have appeared in Southeast Asia and elsewhere. As with any emerging industry, the scale, reach, and speed enabled by technology point to increased concentration of activity. This concentration results in economies of scale, leading to higher profits and lower costs.
- Thirdly, industrialization also promotes the third most apparent characteristic: market integration. Like many growing businesses, cyber fraud groups have learned to run multiple scams – such as investment schemes, romance fraud, and sextortion – in parallel and sometimes in combination. Mixing and matching of classic fraud typologies is far from unknown. Furthermore, cyber fraudsters have begun to diversify, competing and/or collaborating with other major criminal sectors; many experts have observed the increasing overlap between human trafficking networks and those involved in industrialized scam operations. The stark but obvious reality is that different segments of the global economy are finding ways to work together and profit, with cyber fraud playing a central role.

These characteristics will become ever more evident in the medium term. GenAI-generated deepfakes, combined with autonomous agentic AI systems, are likely to produce more convincing, highly personalized cyber fraud campaigns, with capacity limited only by available processing power. The expansion of payment systems and the development of crypto will offer an increasing number of laundering options. This process will be helped if different jurisdictions adopt varying approaches to regulating these emerging technologies: criminals always gain from the fragmentation of, and gaps between, national laws and regulations. Industrialization and integration will also persist for some time, as criminal groups find common interests and potential opportunities for joint profit, not only with each other but also with other malicious non-state actors, such as armed militias and terrorist groups, and even malevolent state regimes. This will embed industrialized cyber fraud deeply into local and regional economies, making it more difficult to address without comprehensive political change. Evidence already indicates that this is occurring in Myanmar. The key challenge for governments and institutions will therefore be not only how to respond tactically and operationally to cyber fraud but also how to disrupt a threat network that is technologically adaptable, rapidly expanding, and increasingly integrated into global illicit economies and ungoverned spaces.

Alongside this, however, it is also important to remember how adaptive, innovative, and creative cyber fraudsters can be. The obvious response from the major jurisdictions affected by cyber fraud (many in the West) will be to target core concentrations of activity with a campaign of unilateral and multilateral punitive measures, such as sanctions, law enforcement investigations and prosecutions, and diplomatic pressure on criminal groups' political protectors, possibly even military interventions. This will almost certainly prompt the major cyber fraud groups to diversify and disperse their operations to new regions, seeking remote spaces in sub-Saharan and equatorial Africa, South America, and central Asia. Given the low barriers to entry in cyber fraud, a governmental and regulatory crackdown on current 'market leaders' will also stimulate risk-tolerant new entrants, as criminal entrepreneurs seek opportunities to take a slice of the pie from targeted market leaders. Indeed, 'cyber fraud-as-a-service' (CFaaS) is already a growing feature of the market, with off-the-shelf phishing kits, mule recruitment networks, and crypto cash-out services available to low-skilled criminal actors through dark markets. If the larger cyber fraud concerns are disrupted, CFaaS will likely flourish, and governments, regulators, and businesses will need to be prepared. What this suggests, therefore, is that, given the technological, economic and governmental environment in which business now exists, cyber fraud is not going to be 'solved' as such, but mitigated, managed and contained. This will not happen automatically, and businesses will need to be proactive.

Addressing the cyber fraud challenge

SHARE THIS

From the perspective of regulated firms, cyber fraud is not just another typology:

it cuts across the basic assumptions on which conventional anti-fraud and AML/CFT control architectures have so far been built.

Policies, processes and procedures – not to mention platforms – designed for relatively slow, higher-value, cross-border flows now must contend with high-velocity, low-value, payments initiated outside the institution's line of sight. The rise of APP fraud is emblematic of this reality.

The overall challenge has multiple dimensions. As alluded to, the core issue is tempo. Fast payments are a customer priority, but they compress the business's window of opportunity for detection and recall from days to minutes, or even seconds. Then there is the problem of authorization. Many of the most damaging cyber frauds will initially appear as fully customer-authorized transfers to apparently legitimate beneficiaries, satisfying control requirements. That a crime has occurred only becomes obvious when the customer themselves realizes and the financial institution investigates, which can take some time, or if a financial institution 'zooms out' and looks at broader patterns of activity hitting its client book.

Being able to do that, moreover, is hard. There are capability constraints. Many institutions struggle to recruit and retain staff who can interpret network analytics, tune fraud-detection and transaction monitoring platforms, and understand upstream cyber vectors while also navigating consumer protection obligations. Finding the right kind of platforms and data in a diverse regtech market is also challenging. Layered over this is internal fragmentation and siloing. Within businesses, fraud, AML/CFT, sanctions, and cyber functions have developed separately, each with its own systems, data lakes, alerting mechanisms, and reporting lines. This means that in many businesses, the team handling the initial report of a fraud will not be the team that also reviews the transactions monitoring alerts arising from the fraudulent funds being moved through networks of mule accounts. While several financial services providers have sought to break down these barriers, it has proved a challenge – especially in the legacy banks.

Furthermore, such fragmentation and siloing are built in across the entire financial ecosystem: between financial institutions, between the public and private sectors, between regulators, FIUs, and law enforcement, and between states. No one stakeholder in the ecosystem has anything like a 'god spot,' where the overall pattern can be seen from a commanding height. This has become increasingly evident as fraudsters have learned to 'hop' between the chains of various types of crypto assets and between crypto and fiat currencies (and back again), leveraging the undulating, confusing landscape of different national crypto regulatory regimes to their advantage. Moreover, even if developing a 'single view' of the problem were possible, not every stakeholder is able or willing to contribute, either due to a lack of awareness and understanding, cost concerns, legal constraints, reputational worries, or regulatory and political agendas. The cumulative effect is a structural mismatch, with the cyber fraudsters being able to tap into the benefits of technological advances, without facing the downsides inherent in running a legitimate, regulated business.

What does this mean for my firm?

Closing the gap requires architectural (rather than incremental) change, an agile approach to technology, and a conceptual revolution in thinking about fraud:

1. **Treat cyber fraud as a financial crime risk.** Firms should treat cyber-enabled fraud as a core financial crime risk, not simply an operational or customer service issue. That means integrating cyber fraud scenarios into enterprise-wide and product-level risk assessments. Boards and senior management should receive regular information on fraud losses and the cyber vectors driving them.

2. **Take a unified approach.** Breaking down fraud–AML–cyber silos means building a unified data layer connecting CDD/KYC, transaction data, fraud, AML and sanctions alerts, and cyber telemetry, including IP location intelligence. On this foundation, firms can create 'fusion' models, uniting diverse teams within one operational framework with a shared data 'spine,' tech stack, and priority list.

3. **Strengthen digital onboarding and identity controls.** Hardening these is essential through the deployment of e-IDV and liveness checks (with anti-deepfake capabilities) plus device, IP and behavioural risk scoring. Applicants for new products should be screened against sanctions, politically exposed person (PEP), and adverse media lists, plus internal (and industry, where available) fraud data and cyber intelligence. Higher-risk customers, especially those with crypto involvement, should be subject to enhanced due diligence (EDD) procedures and, where appropriate, blockchain-analytic monitoring.

4. **Apply friction strategically.** Uncomfortable though it might be, firms need to reshape the customer journey to introduce 'dynamic friction' for high-risk clients and payments. This could include confirmation-of-payee checks and warning screens that reference current scams, cooling-off periods, payment limits for new customers, and additional verification measures for large corporate payments or sudden changes to supplier details.

5. **Leverage AI-driven RegTech.** Legacy tools, driven by static rules, batch reporting, or simple name-matching techniques, cannot address modern cyber fraud. AI-driven anomaly detection, behavioral analytics and network/graph techniques have been shown to improve performance. Strong governance should accompany changes, including integrating human oversight, particularly where automated decision-making impacts customer experiences.

6. **Update investigations and SAR reporting.** Businesses need to consider how generative, agentic, and predictive AI can 'flatten the mountain' of alerts and create more effective investigations. AI-driven 'co-pilots,' intelligence packages and assessment narratives to help with triage, investigations, and SAR drafting processes should also be considered. Businesses should engage with FIUs and law enforcement, and prepare for real-time payment freezes and contingency management during major cyber fraud events.

7. **Build cyber fraud awareness.** Human and cultural dimensions are critical. Frontline staff, relationship managers, and those operating in financial crime 'fusion' teams should be briefed on fraud typologies, drawing on material from the FATF, national FIUs and law enforcement agencies. Incentives for sensitive escalation of suspicious instructions might also be introduced to ensure risk awareness has equal weight with anxieties about introducing friction into the customer experience.

8. **Leverage external knowledge and partnerships.** Information-sharing needs to move from an aspiration to a practice. Participation in national public–private partnerships and fraud-intelligence exchanges (both public and private) should be leveraged to better understand current trends and patterns and gain operational and tactical intelligence on fraud and scam typologies. Professional bodies like ICA and ACAMS are another source of knowledge.

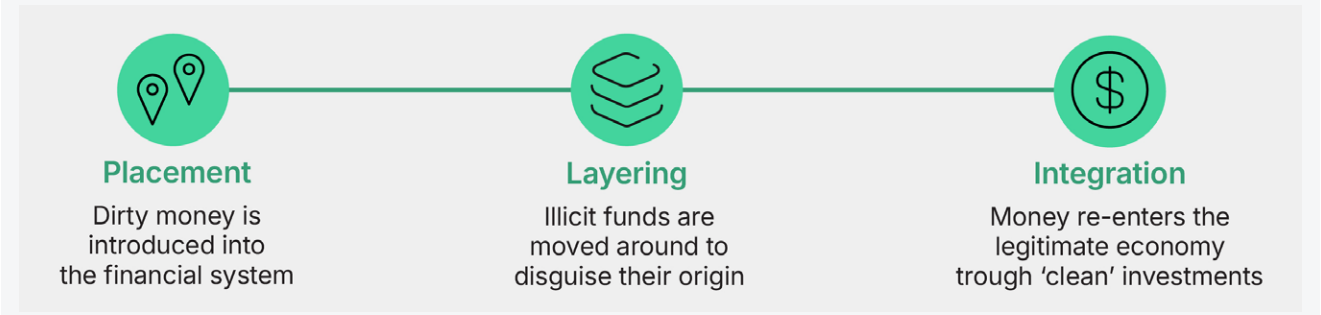
Cyber fraud is the primary manifestation of cybercrime for most citizens and firms. It is scalable, profitable, and intertwined with a range of 'real-world' predicate offenses and money laundering typologies. Its medium-term trajectory – driven by AI, instant payments and industrialized scams – points towards greater volume, sophistication and cross-border complexity, unless upstream controls and systemic responses improve. Companies must re-engineer fraud, AML/CFT, sanctions, and cyber capabilities to address the problem by investing in AI-enabled platforms and developing a culture that sees cyber fraud as a shared threat.

Iain Armstrong
Executive Director, FCC Strategy, ComplyAdvantage

The rise of money laundering-as-a-service (MLaaS)

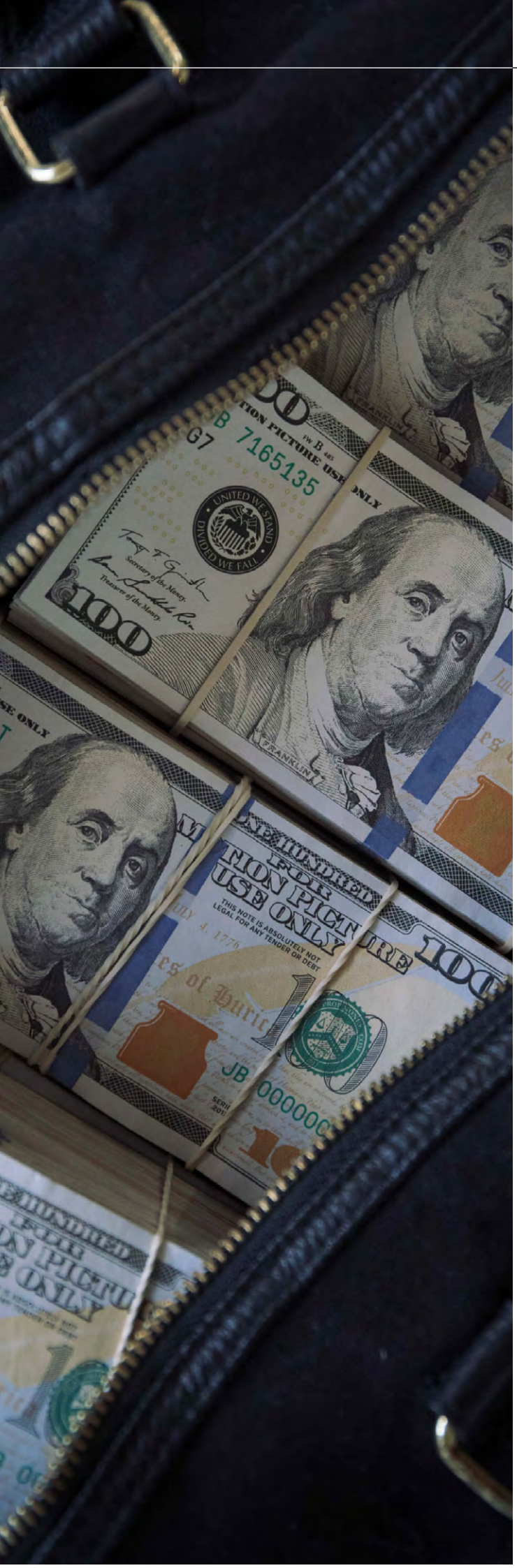
Cyber fraud, like all other serious and organized crimes, aims primarily to generate revenue. However, once that revenue is generated, criminals find it difficult to use it within the legitimate financial system without raising suspicion. It requires cleaning, through a process often mentioned earlier in this section on financial crime: money laundering. Experts generally see this process as consisting of three stages:

- **Placement:** First, funds must be secretly placed into the financial system without detection.
- **Layering:** Next, these funds must circulate undetected within the legitimate financial system for a time, often moving between accounts, various payment channels, and different mediums of exchange (such as fiat, crypto, or value transfer systems like Hawala).
- **Integration:** Finally, the funds are used in a 'legitimate' transaction, buying commodities, assets, or other products, at a point where the connection back to the source of the money is so obscured that it cannot be traced. Or at least, that is the launderer's hope.



Many well-known laundering typologies are used at different points in the cycle: during placement, so called 'money mules' – effectively criminal stooges – are often used to deposit funds into multiple accounts in amounts unlikely to arouse detection (known as 'smurfing'); during layering, funds can be 'cash couriered' overseas, swilled through the accounts of offshore accounts corporate vehicles, or moved in a process known as trade-based money laundering (TBML), where under- and over-invoicing are used to transfer value internationally between criminal counterparties; and during integration, 'high-end' money laundering is regularly used to convert illicit funds into significant assets, such as property, luxury yachts and cars, and a like. However, these are just a selection of the techniques used, and the range of possibilities open to launderers is limited only by their inventiveness.

Since trust is in short supply in the criminal world, larger organized crime groups have historically tended to organize their laundering through 'in-house' facilitation, to keep it under constant scrutiny. In contrast, many individual criminals or smaller criminal gangs have 'outsourced' their laundering to professional facilitators, including corrupt professionals in accountancy and law: think, for example, of the money-laundering lawyer Saul Goodman in *Breaking Bad* and *Better Call Saul*. However, over recent years, the importance of professional money laundering has grown significantly, breaking down the barriers between how serious organized and petty criminals handle their illicit funds. Increasingly, even large and established transnational crime groups are turning to external, specialized laundering networks for laundering on a vast scale. In effect, their needs have helped create a new illicit service industry: 'money laundering-as-a-service (MLaaS).'



The MLaaS landscape

MLaaS is essentially the industrialization/marketization of professional money laundering: specialized groups, networks and platforms that sell laundering capacity as an on-demand service to other criminals. As with any other large industry or market, there are two sides: service providers with distinctive offerings and clients with bespoke needs. Research into the inner workings of money laundering is a tricky and risky business. There is, therefore, a lot that we do not know. However, enough information has emerged from legal enforcement actions such as the NCA's Operations Venetic and Destabilize, official assessments such as Europol's SOCTA, and research, to indicate the existence of five clusters of professional laundering 'service providers.'

1. **The independents:** Some professional money launderers operate as free agents. Some of the independents are pure facilitators, unencumbered by any broader responsibilities. The value of these operators typically lies in their power to orchestrate various elements, stitching together their own mule recruiters and networks, multiple bank accounts and a stable of complicit professional enablers. Other independent operators use cash-intensive businesses, such as bars and restaurants, car washes, and convenience stores, as cover, through which they can co-mingle illicit and licit funds. Another common type of independent professional launderer operates through money service businesses (MSBs), which provide remittance, currency exchange, informal value transfer services, and increasingly, over-the-counter (OTC) crypto services, all of which provide legitimate reasons to take in and send funds.

2. **OCG money laundering divisions:** Several major organized crime groups (OCGs) now run laundering 'divisions' that sell capacity to others, much like a consultancy. For example, several Mexican cartels offer 'black market peso exchange' services to other criminal groups, and Balkan and Turkish networks offer coordinated cross-border cash couriering and trade-based schemes to European clients. Chinese Triads and Fujianese groups offer cash-couriering, commodity trade fraud, and underground banking to global clients, while several West African fraud networks manage laundering circuits that others can access. Cambodian, Lao and Myanmar scam compound operators have also expanded their laundering operations to provide laundering channels for external actors.

3. **Dedicated laundering networks:** Alongside OCG laundering services, there are also dedicated criminal laundering networks which do nothing but launder money. The best-known types of dedicated networks at present are the Chinese money laundering networks (CMLNs), which have become a staple subject of US law enforcement and regulatory notifications in recent years. However, they are not the representatives of this kind of professional launderer, and other groups – several of them Russian – have emerged in recent years. These networks often heavily exploit informal channels such as cash couriering, informal value transfer systems such as Hawala and fei ch'ien ('flying money'), and increasingly, crypto. Although some groups are multinational in character, others operate primarily within one ethnic, linguistic, or cultural group, especially where those groups have a large international diaspora.

4. **Professional services enablers:** Some money laundering providers operate from within the professional services sector, using their public legitimacy as lawyers, accountants and consultants to provide illegal financial services to criminals. Company-formation agents and trust/corporate service providers (TCSPs) have been of particular concern to authorities in recent years due to their ability to establish legal structures, such as offshore shell companies and trusts, recruit nominee directors, and expedite bank account openings with reputable financial institutions. They are particularly impactful providers in this market because of the façades of legitimacy they can build and the reputational cover they can offer, often making them 'high-end' service providers to oligarchs and other high-net-worth individuals seeking to move or protect their assets.

5. **Platform-based networks:** The newest elements in the market are platform-based providers, primarily – but not exclusively – operating in the crypto space. Some crypto mixers and tumblers now operate on subscription models, offering automated cross-chain swapping and other privacy-enhancing tools. Offshore crypto exchanges and over-the-counter (OTC) brokers operating in high-risk and/or poorly regulated jurisdictions add another component and appear to have played integral roles in handling the proceeds of ransomware attacks, cyber fraud, and dark market transactions. Additional players include rogue FinTechs with intentionally weak CDD/KYC frameworks, as well as online gambling operators based in locations such as Curaçao, the Philippines, Cyprus, and parts of Eastern Europe, who provide rapid payouts for successful 'bets' and fiat/crypto conversion facilities.

The result is thus a layered, hybridized service economy, ranging from small-scale facilitators and networks to extensive and growing international enterprises. Each provider will offer its own 'menu' of services, depending on its size and technical knowledge, ranging from independents focusing on placement and layering to 'one-stop shops' that provide end-to-end services to crypto launderers who add a 'plug-in' element within a larger laundering chain. Given the range and diversity of service providers, they can also have a broad spectrum of customers, from small-time criminals working with local independents to massive transnational OCGs seeking a full suite of services. At present, the most significant focus in law enforcement and regulatory circles is on the connection between Mexican cartels and CMLNs, with the former increasingly outsourcing their laundering needs to the latter. However, CMLNs have also been rising in prominence in Europe, as noted in recent research from the think tank RUSI; CMLNs are willing to work with a broad spectrum of clients, regardless of nationality, as long as there is a clear business case for doing so. However, other groups of professional launderers are also gaining wider attention. The groups running Southeast Asian scam centers, for instance, appear to be offering their own crypto-laundering infrastructure to other criminal and state actors, including North Korean hackers.

The current size of MLaaS, or its relative scale compared to 'in-house' laundering, is impossible to determine. There are no clear or reliable global figures. However, the available evidence suggests that professional money launderers handle billions of US dollars each year. A FinCEN analysis of over 137,000 US SARs filed between 2020 and 2024, released in August 2025, identified US$312 billion in suspicious funds linked to a small number of CMLNs laundering funds for Mexican cartels and other North American criminal clients.

Furthermore, the US Treasury's October 2025 designation of the Cambodian Huione Group, a major player in scam center operations in Southeast Asia, stated that of the US$4 billion laundered by the group between August 2021 and January 2025, at least US$37 million derived from crypto assets stolen by North Korea. While such figures do not suggest that professional launderers yet dominate the laundering world (most assessments estimate the scale of annual global laundering in the *trillions* of US dollars), they do show that they are becoming increasingly important players in a developing market.

To explore MLaaS in more detail, we outline two case studies:

Case study (1): Operation Destabilize

In December 2024, the NCA announced a series of arrests and cash seizures of millions of pounds in the UK and beyond. The investigation, which led to the arrests and seizures, as well as several OFAC designations, was known as Operation Destabilize. The NCA subsequently described it as one of the comprehensive disruptions of a major Russian professional money laundering network to date.

Destabilize had begun looking at the laundering of ransomware proceeds from UK attacks. This led NCA officers to 'Smart,' a crypto network controlled by Ekaterina Zhdanova from Moscow, already known for helping Russian elites move money offshore. They then uncovered a linked, parallel structure, 'TGR,' run by George (Georgy) Rossi, Elena Chirkinyan, and Andrejs Bradens, with a London presence and operational links to Dubai. The NCA discovered that Smart and TGR were – in collaboration – providing customized crypto-laundering services to three core client groups: UK drug and firearms traffickers; ransomware and cybercriminal groups; and sanctioned or politically exposed Russian clients seeking to transfer capital into the United Arab Emirates (UAE), Europe, and the UK.

While a core part of the network's operations involved laundering illicit funds already held in crypto, the most interesting aspect of the operation was the process it used to launder criminal cash generated by 'street crime' in the UK, which followed several stages:

- **Cash couriers:** Three regional cash-courier networks collected bags of illicit cash at petrol stations, service stations, lay-bys and industrial estates.
- **Crypto transfers:** When the cash was registered at one of the courier network hubs (in London, Manchester, etc.), Smart was informed and would then move an equivalent amount of crypto (Bitcoin, Ethereum and Tether) from one of its liquidity pools in Moscow or Dubai, via multiple dispersion wallets and high-risk exchanges, to a wallet where the client could access it.
- **Cash recycling:** The illicit cash collected in the UK was then laundered through various commercial fronts, sold to other criminal groups in need of liquidity, used to purchase crypto in small amounts in the UK, and bulk-couriered out of the UK to jurisdictions such as the UAE, often using commercial travel and cash couriers, where it could be integrated directly into the financial system with greater ease.

As a result, the illicit cash was mainly not directly converted into crypto in the UK and transferred cross-border. Much as in a Hawala-style system, the network largely transferred *value* rather than funds across borders.

According to further announcements, Operation Destabilize has continued throughout 2025, both in the UK and with the support of overseas law enforcement agencies. As of November 2025, 128 suspects had been arrested (and many convicted), and tens of millions of US dollars and equivalent currency had been seized globally.

New revelations about the scope of the network's client base also continued to emerge, with investigators linking Smart to Russian intelligence operations in the UK, including the Bulgarian spy ring run by former Wirecard executive and Russian asset, Jan Marsalek.

Case study (2): Chinese money laundering networks (CMLNs)

Over a little more than a decade, CMLNs have moved from the margins of Western law enforcement and regulatory interest to the center of their attention. In 2025, FinCEN issued a significant advisory on CMLN activities, and various think tanks, such as RUSI, issued detailed analyses of these networks' operations. These analyses show that the CMLNs are rooted in the pre-existing Chinese shadow banking networks – as mentioned earlier – the 'flying money' system, which operates on a similar basis to other IVTSs such as Hawala. However, it is important to stress that although CMLNs are deeply integrated into Chinese shadow banking, they are not synonymous with it. All CMLNs use flying money networks, but not all flying money networks are involved in CMLN operations. Moreover, CMLNs serve not only criminals but also normal Chinese who want to send funds overseas while working around the country's stringent capital control laws. Indeed, the high demand for secure capital flight channels has been a staple of these networks' business for decades.

How do CMLNs operate in practice? Despite increasing interest in investigation and research, our knowledge remains limited, based as it is on insights from official statements, legal actions, and occasional media reports. However, some aspects of how these networks operate are becoming clearer. The operational sequence – somewhat over-schematized – is as follows.

Stage 1: Collecting funds

1. On the **Chinese side,** the CMLN facilitators will use encrypted services such as WeChat to advertise their ability to convert Renminbi into foreign currency (typically US dollars) and to ensure secure access overseas (for example, the US, Canada, Australia, or the UK). The client then pays the Renminbi into an account held by a front company or a trusted individual in China. The network takes a substantial fee.

2. In parallel, **overseas,** foreign criminal groups want to launder large amounts of illicit cash (again, typically US dollars). Working with a local CMLN facilitator, they agree on a commission (usually 1-3%), the jurisdiction in which they would like access to their funds (for example, Mexico), and the currency in which they want to receive it (e.g., pesos). CMLN operatives collect the criminals' cash in bulk and then use large mule networks, cash-intensive businesses or over-the-counter (OTC) crypto brokers to place it into the financial system in the overseas jurisdiction.

Stage 2: The mirror trade

3. On behalf of the **Chinese client,** the CMLN facilitator, based outside China in the client's jurisdiction of choice, makes a transfer from a network-controlled account within that jurisdiction, either to the client's account or to a crypto wallet. Alternatively, they will pay the foreign tuition fees for a member of the client's family, buy an asset on the client's behalf (such as property), or buy gambling chips (which can be cashed out by the client on a foreign trip).

4. On behalf of the **overseas criminal client,** the CMLN facilitator in the criminal client's preferred destination (here, Mexico) releases funds in the desired currency to an account controlled by the criminal client, or pays an invoice for the client (perhaps for the cost of precursor chemicals), or provides a shipment of goods from China which can then be sold in the country.

Stage 3: Settling the books

5. Facilitators across the network maintain **ledgers** to track how funds have moved and where imbalances are occurring between liquidity pools in different locations. Over time, these imbalances are addressed through TBML, 'daigou'- style schemes (in which illicit funds held overseas are used to buy legitimate goods, which are then imported into China for sale), or crypto transactions via wallets controlled by facilitators in different locations.

Trust is vital to CMLNs' operations, and as a result, networks are usually based on family links, local connections, and business ties (known as guanxi), which connect facilitators based in China with others within the Chinese diaspora. Communications run through tightly controlled WeChat groups, and roles are compartmentalized to reduce risk. The networks also rely heavily on diaspora members for cash collection and muling (China's large student population is a significant source of casual muling for CMLNs), as well as for professional access to banks, MSBs, law firms, and casinos, which underpin the overseas cash collection infrastructure.

The attractions of MLaaS

Money laundering expert Kathryn Westmore has written that the CMLN model has "blown away the competition." What, therefore, makes CMLNs – and MLaaS as a whole – such an attractive proposition to criminal clients? Five factors stand out:

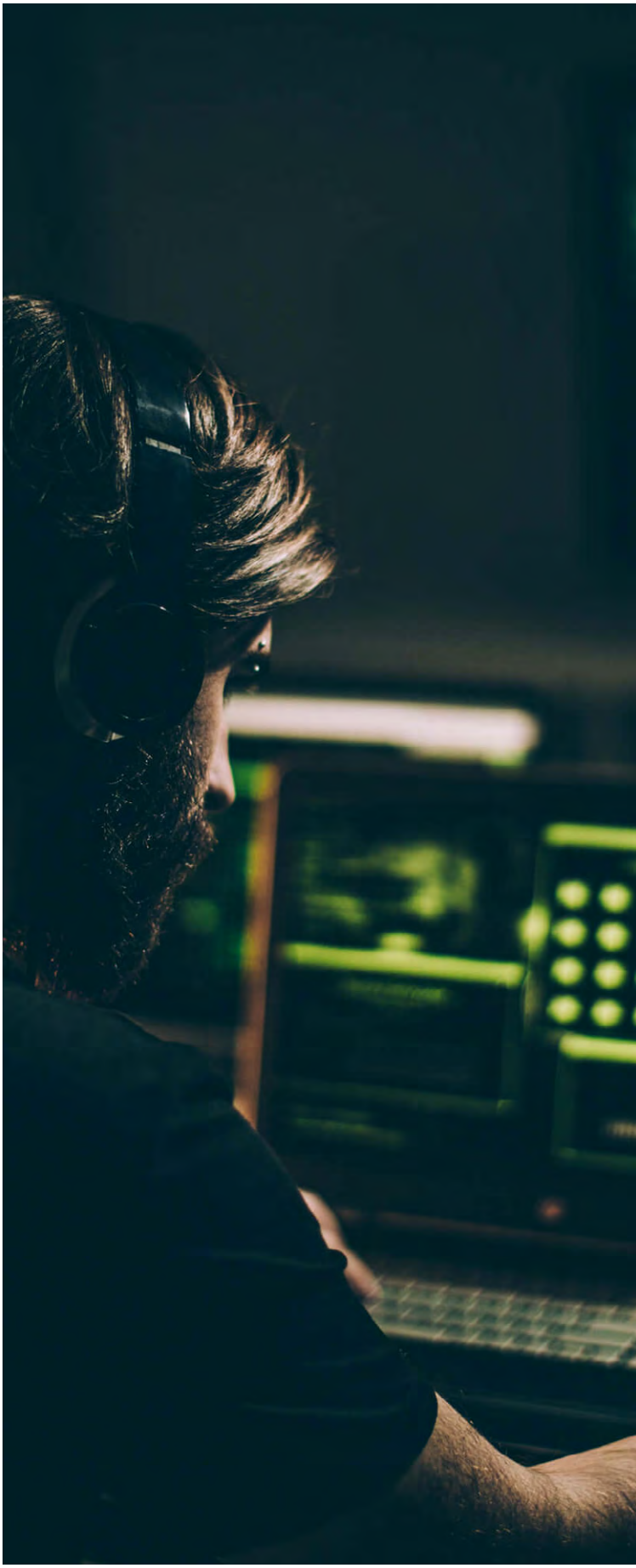
1. **High performance:** With specialization comes high performance. Professional launderers – whether Russian-speaking cash-to-crypto operators or Chinese underground bankers – are experts in what they do and are paid for performance, not loyalty. The need to compete against other providers brings market discipline.

2. **Increased flexibility:** The most successful professional money launderers offer 'plug-and-play' modules: mule-herding, shell-company creation, crypto conversion, cash couriering, etc. These building blocks allow criminals to assemble a laundering strategy that suits their needs without needing any underlying expertise. Criminals can select whichever path fits their risk appetite, geography or required settlement currency.

3. **Reduced risk:** Where in-house laundering increases the risks that law enforcement will make a link to underlying predicate offences, using professional launderers maintains plausible deniability for both the criminal client and the laundering network. Many criminal clients never meet their launderers directly; intermediaries or encrypted channels mediate interactions, protecting group members and complicating criminal charges. Using culturally cohesive groups such as CMLNs also reduces the risk that laundering networks will be infiltrated by law enforcement.

4. **Reduced cost:** Because professional laundering infrastructures are reused, the cost per unit laundered falls, and launderers can charge extremely low rates. As noted by FinCEN Advisory and Westmore's RUSI study, CMLNs launder for cartels at negligible cost, with the profit coming from Chinese clients who pay a premium for offshore dollars.

5. **Increased speed:** Finally, professional launderers are fast. Cash deposited in one jurisdiction can be retrieved elsewhere *within minutes*. In Destabilize, cash pickups in the UK triggered instant crypto movements from Smart's wallets in Moscow and Dubai, reflecting a 'follow the sun' 24-hour settlement model. In the case of CMLNs, cartel clients are reported to have received their funds even *before* the CMLN had completed the upstream settlement.



Professional money launderers are making inroads in the illicit financial ecosystem not simply because criminal groups have decided to outsource a notoriously tricky problem, but because those launderers have built an industry optimized for the vulnerabilities of the modern financial system, and dare it be said, the needs of their clients.

MLaaS trends

The evolution of MLaaS increasingly looks like a structural shift in the organization of illicit finance, one that taps into economies of scale, significant pools of liquidity, and a flexibility of approach not usually seen from in-house launderers. The medium-term trends point to further consolidation and growth of this illicit industry, with key developments including deepening:

- **Industrialization:** MLaaS is likely to consolidate into a smaller number of high-capacity providers operating across various payment rails simultaneously. The trajectory visible in Smart/TGR and CMLNs suggests professional laundering will learn to scale quickly, bringing both efficiency and resilience: networks able to absorb losses, restructure rapidly, and arbitrage between regulatory environments.
- **Hybridization:** Launderers will increasingly treat cash, crypto, trade value, etc., as interchangeable settlement instruments, switching pathways dynamically to avoid detection. Although crypto is sure to become a more significant part of the mix over time, it will not replace other methods but complement and diversify them.
- **Professionalization:** At the lower end of the laundering scale, small-scale self-laundering will persist – local drug networks, low-value frauds, and opportunistic mule schemes. But at higher operational levels, most serious crime groups will increasingly outsource to a handful of professional networks.
- **Technologization:** As in the rest of the criminal economy, AI will almost certainly affect professional laundering, potentially automating mule recruitment, identity fabrication, compliance evasion, and behavioral pattern spoofing. Launderers will also be able to use predictive models to identify low-risk accounts, probe financial institution detection models, and auto-route transactions to minimize detection.

- **Politicization:** The links between Smart/TGR and Russian intelligence indicate that professional money laundering has significant value outside of the criminal world. As geopolitical pressures intensify, states like Russia, Iran and North Korea will look to the most successful MLaaS providers for support in enabling sanctions evasion and supporting clandestine and covert actions overseas. The boundary between pure criminal laundering and state-facilitated illicit finance will become more porous and more challenging for regulated firms with international interests.

Overall, these trends suggest that MLaaS will become more deeply integrated in the illicit economy, evolve rapidly, and become more operationally resilient.

As MLaaS becomes more modular, automated, and globally connected, regulated firms will not only face increasing laundering volumes but also greater difficulty in distinguishing legitimate from illegitimate transactions. The role of the risk management and compliance professional will become much harder.

The MLaaS challenge

And from the perspective of regulated firms, MLaaS is already very hard to detect. First, the link to the underlying crime is barely visible. Most regulated firms only see the laundering layer, which is separate from the drug cartel or scam operation whose funds are being transferred. The entities in front of compliance teams look like regular commercial clients, often with straightforward onboarding documentation and unremarkable declared business activities. The fronts identified in Operation Destabilize – ISM Scaffolding and Sprint Commercial's vehicle exports – appeared to be typical logistics and construction companies that matched local economic activity.

Second, the numerous links within the laundering chain, and those that can come and go, make it hard to identify patterns. Many laundering networks operate through multiple layers, quickly using and disposing of mules and front businesses: easy come, easy go. The students, low-paid workers, migrants, etc., who are exploited by laundering networks typically run low-value, high-turnover accounts, whose behavior superficially matches the broader market profile. Customer-level risk ratings – even when reasonably sophisticated – struggle when the 'customer' is just a disposable node in a much larger patchwork.

Third, MLaaS networks expertly fragment their flows across financial institutions, business lines, product types and countries with the specific aim of undermining traditional monitoring. One institution sees only a sliver of the story, and the red flags that matter – circularity and cross-border connectivity only become visible when multiple datasets are brought together. However, a large portion of regulated firms are not seeing that broader landscape; indeed, even within a single business, relevant risk teams can be highly fragmented, as noted previously.

Fourth, the speed of the modern financial system is a basic challenge in all circumstances. Payments move quickly, as we discussed in our discussion of cyber fraud. But criminal typologies change rapidly too, and the more potential laundering 'modules' that a professional network has at its disposal, the easier it is for them to change their patterns of behavior 'on the fly.' Static, rule-based transaction monitoring frameworks that get changed only periodically are poorly matched to adversaries who can test, learn, and redeploy tactics in days.

Finally, professional launderers are masters at identifying institutional weak links, pivoting towards jurisdictions with weak regulation and supervision and under-resourced FIUs. They also understand how to exploit well-managed international financial institutions too, routing payments through smaller banks before moving them into the broader channels of cross-border correspondent banking, where illicit funds can sit, nested and hardly detectable, in a vast global flow.

The net effect is that MLaaS launders funds through channels that, from a regulated firm's vantage point, often look unremarkable. The consequence is that regulated firms end up trying to detect an adversary whose sophistication, modularity and agility exceed their own. Traditional customer-centric controls, designed for relatively modest laundering operations, usually within single jurisdictions, are poorly adapted to a world in which laundering has become an outsourced, industrial service.

Industry response to MLaaS: The technology & strategy gap

The structural fragmentation, speed, and cross-border complexity of MLaaS require a holistic defensive architecture that moves beyond traditional rules-based monitoring. Our global compliance survey provides key insight into how organizations are meeting this threat and the operational hurdles they face.

Technological adoption: The shift toward advanced analytics designed to counter network fragmentation is widely underway:

- **Behavioral and graph analysis:** More than half of all organizations are currently implementing behavioral analytics (54%) and network and graph analysis (58%) to counter fragmentation and gain a holistic view of suspicious activity.
- **Digital tracing and intelligence:** Firms recognize the need for specialized digital capabilities. When asked about detection capabilities for MLaaS:
  - **Cryptocurrency tracing and forensics:** 35% of organizations currently utilize this capability, with a further 45% planning to implement it within the next 12 months.
  - **Dark web and open-source intelligence (OSINT):** 37% of firms currently monitor OSINT, and 45% plan to adopt this within the next year.

The implementation gap: The high combined adoption rate for technologies like crypto tracing (80% currently using or planning to use) underscores the industry's strategic understanding of the threat. However, the fact that a large portion of these organizations are only in the "planning" stage highlights a significant resource and technology integration challenge. The aspiration to master the fluid, cross-asset nature of MLaaS currently outpaces the pace of operational implementation.

Industry collaboration: MLaaS networks thrive by exploiting the structural fragmentation that exists between financial institutions, different jurisdictions, and the public and private sectors. Because no single entity holds the complete transaction pattern, collaborative intelligence sharing is essential to effectively reconstruct the full view of the criminal network. Recognizing this necessity, our survey showed industry collaboration being prioritized as a fundamental countermeasure: currently, 45% of organizations utilize public/private collaboration and information sharing, indicating that structural engagement is underway but that the majority of the ecosystem has yet to fully implement this vital capability. However, with a further 40% planning to adopt this within the next 12 months, the collective commitment is growing.

What specific measures is your organization implementing, if any, to detect and prevent money laundering-as-a-service activities?

Source: ComplyAdvantage, The State of Financial Crime 2026

What does this mean for my firm?

Firms cannot alter these facts. However, there are reasons to believe they *can* do more to increase the operational friction that professional launderers currently face, especially by turning many of the tools they use themselves to their disadvantage. There is much that firms can do:

1. **Recalibrating risk assessments:** Many businesses do not include an explicit MLaaS element in their enterprise-wide risk assessments. As a crucial first step, firms should carefully identify their exposure to high-risk sectors (PSPs, CASPs, casinos and gambling), products (trade finance, correspondent banking), and payment corridors (US–Mexico–China, China–Southeast Asia, Middle East–Southeast Asia, etc.), not only in isolation but as a combined cluster of risk factors suggestive of higher MLaaS risk.

2. **Refocusing CDD/KYC:** EDD is already a must for various higher-risk clients operating in payments, crypto, and trade. This remains a given: firms need to keep looking for classic indicators like high account turnover with minimal physical presence, or transactional patterns that suggest clients are 'pass-throughs' for money coming from and going to somewhere else. However, even when diligence is deep, the scope can be narrow. Businesses, therefore, need to take a broader view of their clients, considering potential links to laundering syndicates; an invaluable but underused tool for this is adverse media screening.

3. **Reconfiguring transaction monitoring platforms:** Businesses with significant potential risk exposure need to take action to ensure their monitoring platforms are configured (and configurable) to detect subtle signs of MLaaS activity. This means paying close attention to official reports, such as the FinCEN advisory on CMLNs, and to reputable news coverage of cases such as Destabilize, and then aligning monitoring scenarios with real-world behavior. Firms on or near the boundary of the crypto world now also need to consider whether they require access to blockchain analytics tools as standard.

4. **Revamping training:** Although professional money laundering is widely recognized as an issue in the risk management and compliance media and among professional associations, the levels of knowledge and understanding of what contemporary MLaaS means in practice remain low. Operational and investigative staff should therefore be trained on MLaaS concepts, typologies and case studies (CMLNs, the role of scam centers, Russian laundering networks). To further stress-test institutional controls, red team exercises could also be deployed to map how specific laundering network typologies might exploit business products.

5. **Recommitting to intelligence-sharing and partnerships:** As emphasized time and again in this section, professional money laundering networks happily cut across all the boundaries that financial institutions, regulators, law enforcement agencies and national governments have put in place to demarcate responsibilities in the fight against financial crime. Although businesses can't stop launderers from doing this, they can mitigate the risks arising by engaging fully in public-private partnerships, sharing intelligence, and participating in fusion projects that seek to identify MLaaS patterns across institutions. As Operation Destabilize strongly demonstrated, no single institution can see the entire picture. Collaboration is essential.

In summary, businesses must recognize that MLaaS is no longer just a metaphor or an idea waiting to become a reality. It is a substantial illicit services market that enables various kinds of malicious actors to engage in criminal and covert activities, and one that has the potential to grow much further still. As an increasingly important element within the broader global illicit economy – becoming indeed, part of its connective tissue – it needs to be the target of concerted effort by the public and private sectors alike if the risks are to be mitigated, and the threat contained. Regulated businesses will need to do their part.

Andrew Davies
Head of Global FCC Strategy,
ComplyAdvantage

STOP THE TRAFFIK

Human trafficking: A critical financial crime risk

BY REBEKAH LISGARTEN, CEO, STOP THE TRAFFIK

STOP THE TRAFFIK is a global organization working to disrupt human trafficking and build resilient communities through intelligence-led prevention. CEO Rebekah Lisgarten, alongside a dedicated expert intelligence team, leads this mission, drawing on over a decade of experience in survivor advocacy and strategic operations to scale preventive systems that protect vulnerable populations worldwide.

Akello's* story

Akello*, a Ugandan national, travelled to Thailand after being recruited for a job. Akello left Uganda with hope in his heart. The journey felt like the start of a brighter future. But the moment he arrived, the dream turned into a nightmare.

He was kidnapped, taken across the border into Myanmar, and trapped in a heavily guarded compound. There, the reality was brutal. He was forced to spend his days conducting online scams, enduring constant abuse.

Akello managed to get a message to STOP THE TRAFFIK, and we helped facilitate a targeted intervention. We mobilized our network, alerting international banks in an attempt to freeze the traffickers' illicit funds and disrupt the financial flows that enable their crimes.

At the same time, we worked with global law enforcement and trusted local organisations, who coordinated an operation to rescue Akello and others who had been suffering alongside him.

The business model of human trafficking

Human trafficking is a crime that involves recruiting, transporting, or harboring people through force, fraud, or deception with the aim of exploiting them for profit. This exploitation can occur within forced labour, commercial sex, or forced criminality, among other forms, as traffickers monetize the suffering of their victims. Unlike organized immigration crime, trafficking does not stop once victims are moved, nor does it require the crossing of borders.

Akello's story shows that modern slavery and human trafficking (MSHT) is not only a serious human rights abuse, but also an illicit business model driven by financial gain. **Scam compounds alone generate US$44 billion annually.** This business model works for traffickers because it is low risk and high reward. **Globally, MSHT generates around US$500 billion a year, yet less than 1% of laundered funds are ever recovered.**

Traffickers move their proceeds through legitimate financial institutions to launder their illicit funds. This means that financial institutions are uniquely positioned to disrupt this global issue.

If illicit funds can be identified and intercepted before they enter legitimate channels, the balance can be shifted, transforming trafficking into a high-risk, low-reward enterprise. By cutting off traffickers' ability to profit from their crimes, exploitation can be prevented before it occurs.

$498bn

APPROXIMATELY GENERATED ANNUALLY IN CRIMINAL REVENUE BY TRAFFICKERS

* Name changed to protect identity

How has modern slavery and human trafficking evolved in the past year?

In 2026, the threat posed by MSHT continues to evolve, as traffickers find new ways to recruit and exploit victims and generate profit.

The exploitation of victims in forced scamming compounds across South-East Asia, like the one Akello was trapped in, has emerged over recent years as a widespread issue. This came to the fore in October 2025, when the US and UK imposed sweeping sanctions on organized crime syndicates in the region, citing forced scamming and cryptocurrency fraud. Among those sanctioned was the Chairman of Prince Holding Group, a major company based in Cambodia that STOP THE TRAFFIK had identified as a suspicious entity months earlier.

Many of these scams involve fraudulent cryptocurrency schemes. While blockchain technology has the potential to deliver unprecedented transparency, the use of anonymous cryptocurrency wallets can also obscure identities. Funds sent and received by unknown entities create significant challenges for due diligence, increasing the risk of illicit activity going undetected and allowing those engaged in exploitation to operate with impunity.

Artificial intelligence (AI) is also reshaping the threat landscape. Traffickers are using AI to scale recruitment and exploitation online and to enable more sophisticated fraud, including deepfake interviews, forged documents, and false job advertisements. At the same time, AI can be used to amass and analyze large datasets, enabling organizations to identify emerging typologies, detect patterns, and stay ahead of traffickers.

50m PEOPLE ARE HELD IN MODERN SLAVERY GLOBALLY

$44bn

GENERATED ANNUALLY BY CYBER SCAM COMPOUNDS IN MEKONG COUNTRIES

UNITED STATES INSTITUTE OF PEACE, 2024

What does this mean for my business?

As the regulatory and risk landscape continues to change, it is essential for firms to remain alert to evolving requirements and to stay ahead of bad actors seeking to move illicit funds through their organizations. In 2025, several major financial institutions only discovered weaknesses in their systems, policies, and due diligence frameworks after facing significant fines and penalties. Acting preventively to identify red flags and mitigate risk is a far more effective approach.

Organizations must prepare for the emerging threats and challenges that will shape trafficking patterns, ensuring their response remains effective.

Robust know your customer (KYC) due diligence is essential, as onboarding presents a critical opportunity to identify risk. When red flags are missed at this stage, identifying suspicious activity later in the customer lifecycle becomes significantly more difficult. Effective transaction monitoring is also vital to detecting and responding to suspicious individuals and entities in real time.

An intelligence-led approach enables institutions to move beyond reactive compliance, strengthen risk assessments, and respond earlier to emerging threats. Effective information sharing, both within organizations and across the sector, is critical to disrupting modern slavery and human trafficking. Shared intelligence can provide the missing link that enables earlier intervention and helps prevent cases like Akello's from occurring in the first place.

Back to beginning
Previous section
Next section

Geopolitics and sanctions

Year of the rift

The growing geopolitical fragmentation of previous years continued in 2025. Despite the newly returned President Trump's expressed desire to bring peace to the world's various conflicts, the US found itself embroiled in military action against Iran, alongside Israel, in the summer. At the same time – and despite ongoing peace initiatives – Russia's war in Ukraine remained unresolved, and differing attitudes towards the war, and to China's rise, widened rifts among liberal democracies. Conversely, the loose coalition of states aiming to revise the Western-led order – notably China, Russia, Iran, and North Korea – continued to assert themselves. Among them, only Iran suffered significant setbacks, following Israeli and US military action.

In this environment, Western states continued to apply sanctions – measures to restrict transactions with designated firms, banks, and individuals – to respond to violations of international norms. The EU, UK, and other partners introduced new sanctions packages against Russia's war effort and aimed to restore suspended UN sanctions targeting Iran's nuclear programme. However, these efforts were undermined by increasingly sophisticated sanctions evasion, using third-country transshipments and a massive global 'shadow fleet.' Middle powers such as Turkey and India also avoided complete alignment with Western measures, making implementation harder still. Even the United States showed a reduced appetite for multilateral sanctions action, instead using its designatory powers most heavily against so-called 'narco-terrorist' cartels in the Americas. At the same time, the Trump administration showed a distinct preference for unilateral tariffs as its primary tool of coercive statecraft.

The fragmentation of sanctions regimes and the rise of sophisticated evasion networks have thus placed businesses in a difficult position in 2025. On one hand, governments and regulators are harder to satisfy. The proliferation of autonomous national sanctions regimes has increased the risk that multinational firms will be caught in the crossfire of conflicting rules and regulations. Equally, the sheer volume and range of new measures have shifted greater compliance responsibility onto the private sector, resulting in heightened political, legal, and regulatory risks, as well as rising compliance costs for firms.

Global hotspots

In this first section, we focus on the major geopolitical events of the past year and the financial and economic measures that governments have taken in response.

The Middle East: Israel versus 'The Axis of Resistance'

Following the attack by the Islamist group Hamas on Israel on October 7, 2023, Israeli armed forces conducted sustained and devastating military and covert operations against Hamas in the Gaza Strip, and two other major partners in the Iran-led Axis of Resistance: the Shia Islamist group Hezbollah in southern Lebanon, and the Houthis, an armed militia professing a variation of Shia Islam, in Yemen.

2025 began with the war in Gaza ongoing, the Lebanon conflict subject to a ceasefire agreed in November 2024, and the Yemen front relatively quiet. Although Western states continued to show broad support for Israel in Gaza, they also expressed increasing concern about the impact of the conflict on Palestinian civilians in Gaza and the conduct of Israel's military. According to the World Bank, the ongoing war was causing "economic paralysis" in Gaza and a "deep recession" in the West Bank, forcing many Palestinians to operate outside its formerly cash-based economy; according to the Bank's figures, severe cash shortages resulted in a "massive surge" in the use of e-wallets, with outstanding e-wallet balances exceeded $40 million in February 2025.

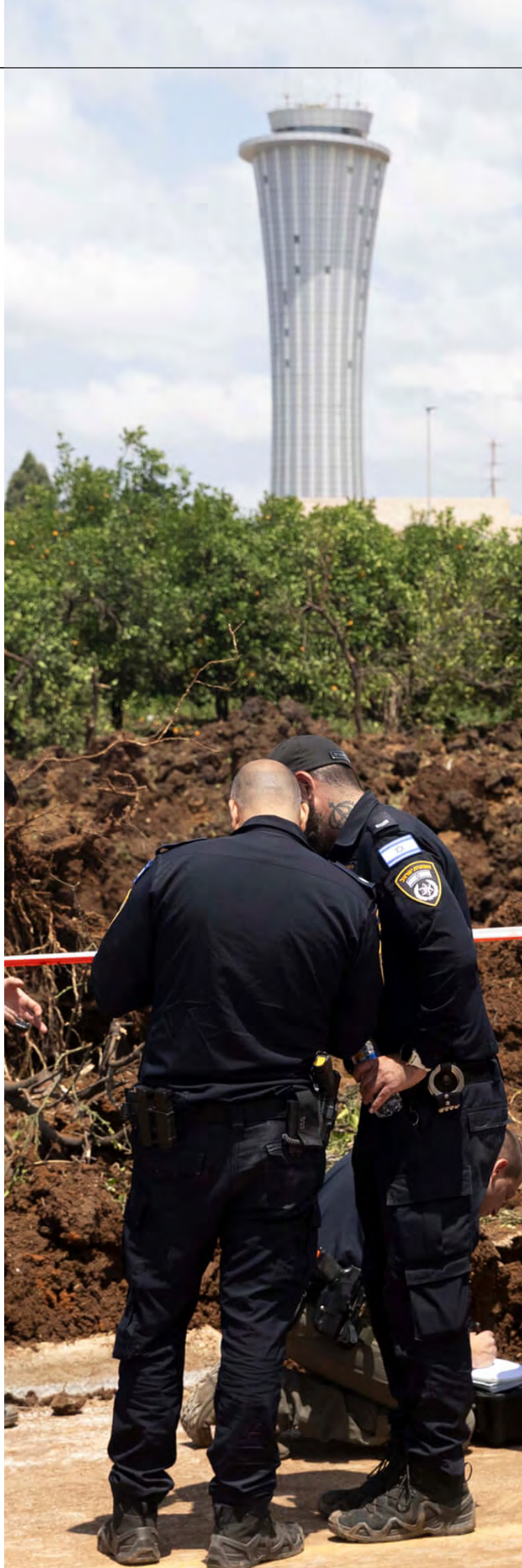
Outside pressure from the US and Arab states, including Jordan, Egypt, and Qatar, initially led to a limited truce agreed between Israel and Hamas. Starting on January 19, the ceasefire brought about a period of de-escalation in Gaza, several rounds of hostage exchanges, and the delivery of some humanitarian supplies. However, amid claims of violations from both sides, the deal collapsed on March 18, when widespread Israeli airstrikes took place across Gaza.

Although negotiations resumed in the summer, progress proved difficult, and the talks came close to collapse in the wake of an unprecedented Israeli airstrike on Hamas's political leadership in Doha, Qatar, on September 9. Qatar, the US, and others remained committed to mediation, however, and a month later, on October 9, Israel and Hamas agreed on a further phased ceasefire and hostage-release schedule at Sharm el-Sheikh in Egypt. As the year ended, the truce continued in theory. However, its implementation remained highly uneven, with both sides claiming that the other had infringed the deal's terms.

In Lebanon, a period of relative calm early in 2025 was disrupted by Hezbollah with a barrage of rocket fire into northern Israel in March, prompting Israeli retaliation.

Israel conducted airstrikes against Hezbollah's military infrastructure throughout the summer, focusing on the group's drone production facilities around Beirut and its elite unit training sites in the Bekaa Valley. The pattern continued into autumn, with a wave of Israeli airstrikes on November 6 in southern Lebanon. The conflict had returned to a familiar historical rhythm of sporadic outbursts of attack and counter-attack.

In Yemen and the Red Sea, a similar pattern unfolded. 2025 began quietly, with the Houthis promising in January to target only Israeli-affiliated vessels in the Red Sea if the Gaza ceasefire held. However, in the same month, the US reclassified the Houthis as a Foreign Terrorist Organisation (FTO), and in March, it launched significant airstrikes against the Houthis' missile and drone sites, leadership, and fuel infrastructure. US strikes continued into April, including an attack on the Ras Isa fuel terminal, with the UK taking part in assaults on Houthi drone sites at the month's end. In May, the Houthis responded with a missile attack on Ben Gurion Airport in Jerusalem, prompting Israel to retaliate with air strikes on the port at Hudaydah and Sanaa Airport in Yemen. The US ended its own air attacks in the same month, following an Omani-brokered truce, yet military actions persisted between the Houthis and Israel; the Houthis resumed maritime assaults on commercial vessels in the Red Sea and missile strikes against Israel, to which Israel responded with a series of aerial attacks in late summer and autumn against Houthi military sites and senior figures, including one that killed the Houthis' military chief of staff, Mohammed al-Ghamari, in October. Slightly chastened, the Houthis announced a unilateral ceasefire against maritime targets and Israel alongside the Gaza ceasefire. However, tensions remained high, with the group making new threats against Saudi Arabia in November. Yemeni affairs were further complicated in December when the Saudis launched air strikes on the Yemeni port of Mukalla, held by a southern Yemeni militia with separatist ambitions. The group – the Southern Transitional Council – was supported by the United Arab Emirates (UAE), who were themselves allies of the Saudis against the Houthis. As in other parts of the region, forthcoming developments remained uncertain, and the 'peace' fragile and uneasy.



Sanctions against the Axis of Resistance

Although the US and the UK used military action against the Houthis, Western countries have preferred to use sanctions against the terrorist groups and militias of Iran's Axis of Resistance. In recent years, there have been signs of growing coordination among them on such measures; however, 2025 has shown some intriguing variations in approach.

In the case of all three 'targets' – Hamas, Hezbollah and the Houthis – the US remained the most active designator. As in previous years, the US has been eager to target the financial infrastructures underpinning the groups' operations. In June, the US Treasury's sanctions unit, the Office for Foreign Assets Control (OFAC), announced sanctions on what it described as 'sham' charities and their facilitators, alleging that they had helped finance Hamas's military operations under the cover of humanitarian assistance. This was followed in early July by designations of seven individuals and one entity linked to the Hizballah-controlled financial institution Al-Qard Al-Hassan (AQAH), which came as part of a broader, ongoing US effort to disrupt sanctioned Iranian oil sales and illicit financial flows between Iran and Lebanon. In early November, John Hurley, the Undersecretary for Terrorism and Financial Intelligence at the US Treasury, signaled that this campaign would continue, saying that this was the "moment" to untether Hezbollah from its Iranian financial lifeline. Three Hezbollah financial facilitators allegedly involved in using Lebanese exchange houses to funnel Iranian funds to the group were sanctioned in parallel.

The United States also issued multiple designations against the Houthis' financial networks throughout the year, starting with the sanctioning of the Yemen Kuwait Bank in January, for alleged involvement in laundering Houthi funds and facilitating transfers to other groups such as Hezbollah. Additional measures throughout the year included designations of senior Houthi officials involved in weapons procurement from suppliers in Russia, China, and Iran; various vessels and ship owners engaged in shipping oil and refined petroleum to finance Houthi operations; and networks of individuals and businesses involved in petroleum smuggling and money laundering for the Houthis.

One of the most significant rounds of US action came in September, when OFAC targeted an extensive multi-purpose network operating in Yemen, the United Arab Emirates (UAE), China and the Marshall Islands, involved in weapons procurement and oil smuggling.

In comparison, the EU, UK, Canada, and Australia imposed far fewer new designations against the three groups in 2025, instead sustaining existing measures.

In January, the EU renewed its existing sanctions against Hamas, and in July, it maintained the terrorist listing of Hamas's military wing and Hezbollah. Despite demands from the Netherlands in October, the EU did not designate the Houthis as a terrorist group. The UK and Canada maintained their proscriptions of Hamas and Hezbollah but took little additional sanctions-related action against either, or the Houthis. Australia also relisted Hezbollah and Hamas as terrorist organizations under counter terrorist financing (CTF) legislation in September, while imposing additional sanctions on three individuals and one entity linked to Hamas fundraising.

The question of Israel

Following the attacks on October 7, 2023, Western liberal democracies reaffirmed Israel's right to self-defense and focused on condemning Hamas. However, as Israeli military operations in Gaza intensified and civilian casualties increased, humanitarian conditions deteriorated, and Western officials became more critical of the Israeli military's adherence to international humanitarian law. Simultaneously, several Western governments expressed concern over the violent treatment of Palestinians in the West Bank and the expansion of Israeli settlements, which they believed would jeopardize the prospects of a future "two-state" solution to the Israel-Palestine conflict. This prompted several governments and authorities, including the US, the UK, the EU, Canada, and Australia, to impose sanctions on those allegedly responsible for settler violence, while some also restricted arms supplies to Israel.

Western criticisms of Israeli conduct persisted into 2025, with the UK imposing sanctions in May on the prominent settler spokesperson, Daniella Weiss, two illegal West Bank outposts, and two settler support organizations. The following month, on June 10, the UK joined Australia, Canada, New Zealand, and Norway in announcing coordinated sanctions against two far-right Israeli cabinet members linked to the settler movement, Itamar Ben-Gvir and Bezalel Smotrich. Several Western governments also began reassessing their trade relations with Israel. In May, the UK paused negotiations on a new trade agreement, and in September, the European Commission proposed reviewing and potentially suspending Israel's status as a preferred trading partner within the EU, as well as sanctioning Israeli cabinet ministers and the infrastructure supporting the settler movement. These proposals sparked controversy and were not approved by all member state governments. Most importantly, however, several Western governments, including the UK, France, Canada, and Australia, decided to recognize Palestine as a sovereign state in September. Although largely symbolic, this move sent an unprecedented signal of how much many Western governments had shifted their stance since autumn 2023.

Alongside these developments in the West, 2025 also saw numerous governments in the Asia-Pacific region, Latin America, and Africa increase their criticism of Israel. The toughest measures came from Singapore, which announced sanctions on leading Israeli settlers in September; the Singaporean government also recognized the Palestinian state in parallel. Earlier in the year, in July, the Hague Group – a coalition of eight countries (Bolivia, Colombia, Cuba, Honduras, Malaysia, Namibia, Senegal, and South Africa) – organized a conference in Bogotá, Colombia, to discuss what they viewed as Israel's gross violations of international law. This resulted in the 'Bogota Declaration,' signed by the original eight members of the group plus four additional countries, and later joined by a fifth, which committed the signatories to restrict arms exports to Israel, review trade and procurement relationships, and support cases brought against Israel and Israeli leaders under international law (two of which were ongoing at the International Court of Justice [ICJ] and the International Criminal Court [ICC]).

The most significant state holding out against criticism of Israel remained the US. The decision of the ICC in November 2024 to issue arrest warrants for Israeli Prime Minister Benjamin Netanyahu and former defense minister Yoav Gallant had been declared "outrageous" by then-President Joe Biden (neither the US nor Israel are members of the court). His successor had a similar, but more confrontational, response: in February 2025, President Trump issued an Executive Order granting him the power to impose sanctions on members of the ICC itself, declaring that the warrants against the Israeli leaders exceeded the court's legitimate authority. The ICC Chief Prosecutor, Karim Khan, was designated as a first step, to be followed by two deputy prosecutors, six presiding judges, the UN Human Rights Council's Special Rapporteur on Palestine, and several non-governmental organizations (NGOs) working with the court on Palestinian issues. These moves were very much in keeping with past Trump actions – in his first term, he had imposed sanctions on senior ICC figures investigating alleged US war crimes in Afghanistan – but this time, the measures were more comprehensive in scope; indeed, in September, US media outlets suggested that there was a genuine possibility that the Trump administration might sanction the ICC as an entity in its own right.

The Middle East: Iran

Since the Iranian revolution of 1979, the relationship of the Shia religious regime in Tehran with the US and its Western allies has been extremely fractious. From the outset of the regime's emergence, the US has imposed a range of complex and evolving sanctions targeting:

- Iranian state financial assets, financial institutions, and major private financial institutions.
- Members of the regime, including the Supreme Leader Ali Khamenei and the Iranian Revolutionary Guard Corps (IRGC), the elite military organization subject to the sole authority of the Supreme Leader.
- Iran's oil and gas industry, as well as other key sectors, including transport, shipping and logistics, construction, manufacturing and mining.
- Iran's links to terrorist groups such as Hezbollah and Hamas.
- Iran's military procurement efforts, especially around the development of ballistic missiles and nuclear technology.
- Iran's domestic human rights violations against ethnic, religious and gender-based identity groups.

Separately, from 2006 to 2010, the United Nations Security Council (UNSC) imposed an escalating range of sanctions targeting Iran's nuclear and ballistic missile programs. These measures were in part suspended in 2015, following the agreement of the Joint Comprehensive Plan of Action (JCPOA) between Iran and the permanent members of the UNSC – the US, UK, France, China and Russia – and Germany and the EU. The JCPOA provided for limited sanctions relief for Iran, allowing it to sell oil, subject to the regime's agreement to limits, controls and international inspection of its nuclear program. However, during his first term, President Trump withdrew the US from the deal, reimposed sanctions that had previously been suspended, and launched a campaign of "maximum pressure." Iran and the other parties continued with the agreement, although Tehran's compliance with it seemed increasingly tenuous. The EU, UK, Canada and Australia also created their own autonomous sanctions regimes focused on Iran, which targeted Iran's role as a state-sponsor of terrorism, its abuse of human rights, and its material support for Russia's invasion of Ukraine, primarily through the provision of Shahed drone technology to the Russian army.

Iran enters 2025

The new year began with Iran under significant pressure, both internal and external. Domestically, the regime was still seeking to consolidate itself in the wake of the death of President Ebrahim Raisi in May 2024 (killed in a helicopter crash), with his more moderate replacement, Masoud Pezeshkian, seeking to curb the ultra-conservative instincts of the religious elite. The country also remained under massive economic strain, resulting from decades' worth of sanctions and the regime's economic mismanagement and corruption. This economic discontent exacerbated underlying societal divisions over the rights of women, and the status of minority ethnic and religious groups. Overseas, moreover, Iran faced an uncertain landscape. While political, economic and military ties had continued to develop with Russia and China, the regime faced the return of Donald Trump, who, in his first term, had been a determined opponent of Tehran.

Nuclear negotiations – and war

The nuclear issue was the primary shaper of events in Iran-West relations throughout 2025. Initial Iranian fears about Trump were justified on February 4, when the President signed a new National Security Presidential Memorandum (NSPM) reinstating the "maximum pressure" campaign. At the same time, however, he also sent softer signals to Tehran, expressing willingness to engage diplomatically. In spring 2025, five rounds of indirect Iranian-US nuclear talks took place, with President Trump later claiming he had been genuinely open to sanctions relief for Iran, in exchange for significant concessions. However, by early summer, the talks had effectively stalled. Separately, on June 12, the UN's International Atomic Energy Agency (IAEA) declared that Iran was no longer in compliance with its safeguards agreements.

In this atmosphere of uncertainty, and prompted by what it claimed to be intelligence showing Iran preparing to make a nuclear weapon, Israel acted. On June 13, it launched a wide-ranging and rolling aerial bombardment of Iran's nuclear and military infrastructure, leaders, and scientists. The US joined the air attacks on June 21, targeting Iran's main nuclear sites at Fordow, Natanz and Isfahan. Iran made retaliatory missile strikes against Israel and a US base in Qatar, but by comparison, the damage caused by Iranian strikes was relatively limited. President Trump announced an Israel-US-Iran ceasefire on June 23, claiming that the '12 Day War' had crippled Iran's nuclear program beyond repair.

Outside assessments of the damage done were less optimistic, however, suggesting that even if Iran's program had been set back, it had not been destroyed. Others also noted how the attacks on Iran had strengthened support for the regime, rather than weakened it. Tehran quickly made it clear it would not be cowed, and on June 25, it suspended cooperation with IAEA inspectors. The reimposition of UN sanctions lifted by the JCPOA then unfolded over the summer and autumn. The UK, France, and Germany (known as the 'E3') offered a diplomatic opening to Iran, which Iran in effect refused. On August 28, the three countries therefore formally notified the UNSC that Iran was not complying with the JCPOA and sought to trigger the sanctions "snapback" mechanisms built into UNSC resolutions, which gave the UNSC 30 days in which it could, in theory, stop the sanctions returning, based on a majority vote. Although both Russia and China made efforts to stymie the return of sanctions, there was limited appetite to help Iran across most of the UNSC, and the restrictions against Iran re-entered into force on September 27. This development required all UN members to reinstate

the sanctions, and the EU, the UK, and other Western states took the necessary legal steps to implement them. Russia, however, refused to comply, declaring the move "illegal," while China, somewhat more circumspect, continued to call for a diplomatic solution. In the autumn, Iran made several diplomatic overtures towards the US, but these did not lead to any substantive developments by the end of the year. Indeed, as public protests in many Iranian cities over the state of the economy erupted in late December, tensions rose again between Tehran and Washington, as the Trump administration warned the regime not to use force. As 2026 began, many observers were actively speculating that another round of US military – and possibly Israeli – military action against Iran was increasingly likely.

Other sanctions against Iran: The US

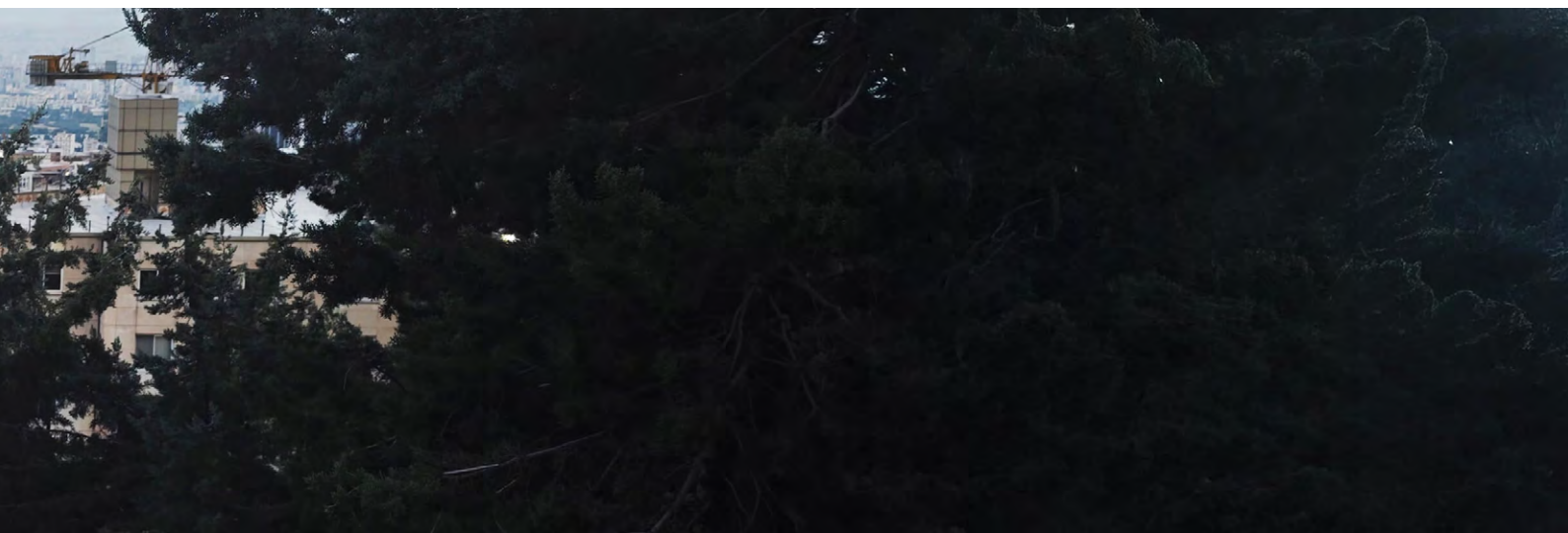
With the nuclear issue as the primary focus in 2025, the media paid less attention to other changes to Western sanctions regimes. However, this was not due to a lack of activity. The US was the most proactive, implementing dozens of new restrictions targeting five broad areas of Iranian activity, covering the regime's:

- Illicit hydrocarbon sales.
- Illicit military procurement efforts.
- Operation of a shadow financial system.
- Global covert and intelligence operations; and
- Support for terrorist and militia groups across the Middle East.

Some of the most aggressive US actions focused on Iran's oil and gas sales. Successive packages throughout the year reinforced and extended past US designations, targeting Iran's key individuals and firms within Iran's oil production and export infrastructure, the global 'shadow fleet' of tankers moving Iranian oil, the various front companies, financial and logistical intermediaries in Iraq, the United Arab Emirates (UAE), India, Hong Kong (often expatriate or dual national Iranians or Iraqis) that facilitate its sale, and the commercial consumers in countries that have been willing to buy Iranian oil, whether wittingly or otherwise. Of note in 2025 was a strong US focus on independent 'teapot' refineries in China (see, for example, Luqing Petrochemical in March, Shandong Shengxing Chemical in April, Hebei Xinhai Chemical Group in May and Shandong Jincheng Petrochemical Group in October).

The US also continued to target Iran's weapons procurement. The US designated various targets which it assessed to be supplying the regime with propellants, electronics, machinery, and dual-use components that could be used in its weapons programs. A notable example occurred in November, when OFAC designated 32 individuals and entities within an extensive procurement network based in Iran, but spanning China, India, Europe, and the Middle East. Iran's nuclear program was also subject to further measures; OFAC designated several companies supporting Iranian centrifuge development in April, and the State Department individuals and institutions involved in Iranian nuclear research and development in May. A further notable US action which foreshadowed future events came at the end of December, when OFAC sanctioned Iranian and Venezuelan individuals and companies linked to Iran's supply of drone technology to the Maduro regime in Caracas.

The third important area of US action was Iran's shadow financial system. New designations targeted foreign exchange brokers, remittance providers, Hawala dealers (Hawala is a traditional value transfer system widely used across the Muslim world), and third-country banks that Iran has used to collate, move and then spend many billions of US dollars generated from oil sales.



Notable examples included the June designations of three Iranian nationals – the Zarringhalams – who were alleged to manage a network of exchange houses in Iran and front companies in the UAE and Hong Kong. The US also expanded its actions against Iran's attempts to work around the existing international payments infrastructure, designating Iran's RUNC Exchange System Company and its involvement in the development of the Cross-Border Interbank Messaging System (CIMS), a transactional messaging system designed to help Iran work around its ban from the global SWIFT payments messaging system. The US also acted against Iranian abuse of cryptocurrencies, designating in September two Iranian facilitators, Alireza Derakhshan and Arash Estaki Alivand, who purchased over $100 million in cryptocurrency as part of a scheme to launder funds from Iranian oil sales.

The fourth area of US activity was focused on Iran's intelligence and covert operations. Some designations were historically focused;

in March, the US targeted three officials of Iran's Ministry of Intelligence and Security (MOIS), linked to the disappearance and probable death of Robert Levinson, a former FBI Special Agent who went missing on the Iranian island of Kish in 2007. Others were more contemporary, focusing on recent Iranian covert operations in Europe, which utilized criminal operatives to provide deniability for attacks. Notably, in March, the US designated the Foxtrot Group, a Kurdish criminal gang based in Sweden and its on-the-run leader, Rawa Majid, for attacks on Israelis and Jews in Europe, including a January 2024 attack on the Israeli Embassy in Sweden.

Finally, in tandem with its other actions against Iran's non-state partners in the Axis of Resistance, mentioned previously, the US also targeted these groups' involvement in Iran's illicit financial activities. The Houthis in particular faced numerous designations for their participation in Iranian oil smuggling, weapons and commodity procurement, and financial facilitation, particularly through the network of Houthi financial facilitator and IRGC intermediary, Sa'id al-Jamal. The US also designated several financial institutions linked to Houthi financial activities, including the Yemen Kuwait Bank for Trade and Investment, and the International Bank of Yemen (IBY).

The US turned its attention too to the Shia militias of Iraq, designating four additional Iran-supporting groups – Harakat al-Nujaba, Kata'ib Sayyid al-Shuhada, Harakat Ansar Allah al-Awfiya, and Kata'ib al-Imam Ali – as foreign terrorist organizations (FTOs) in September. This was followed in October by the listing of individuals and companies linked to the Iraqi conglomerate, the Muhandis General Company, which the US alleged helped Iran and its Iraqi militia allies evade sanctions, smuggle weapons, and corrupt Iraqi business, politics and society. Hezbollah – whose joint activities with Iran were already heavily sanctioned – received further attention too, with the designation in November of three of its leading financial facilitators responsible for laundering the proceeds of oil smuggling and $1 billion in IRGC funding, leveraging Lebanon's largely cash-based economy and unlicensed money exchanges and exchange houses.

Other sanctions against Iran: The EU and the Anglosphere

Western institutions and states beyond the US took their own action against illicit Iranian activities in 2025, focusing on the regime's domestic human rights record, its acts of transnational repression, and its support for Russia's war in Ukraine. The EU, for one, took an increasingly assertive posture against Iran. In April 2025, its Council (the EU's central executive intergovernmental body) initiated new restrictive measures against Iranian prison officials and judges, including Hedayatollah Farzadi, the head of Evin prison, and Mehdi Nemati, the head of the Fars Prisons Protection and Intelligence Department, for their involvement in arbitrary detentions.

The EU also designated two Iranian detention facilities: Shiraz Central Prison in Fars and the First Branch of the Revolutionary Court of Shiraz. In July, the EU moved to sanction two Iranian intelligence officers involved in the persecution of dissidents overseas, as well as key members of the Zindashti criminal network, a group used by the MOIS to intimidate and assassinate targets overseas. The summer of 2025 also saw the EU focusing on Iran's supply of drones and missiles to Russia and its partner groups, such as the Houthis, renewing and slightly extending its preexisting sanctions on several individuals and entities in the Iranian defense-industrial establishment for a further year in July.

In the Anglophone West, the governments of the UK and Canada joined the US and EU in applying additional pressure on Iran. In April, the UK designated the aforementioned criminal Foxtrot group in Sweden, as well as its leader, Rawa Majid. In August, the UK also designated the logistical and financial network of Iranian businessman Hossein Shamkhani, which it alleged supported Iranian sanctions evasion. In parallel with its push to reinstate UN nuclear sanctions, moreover, the UK announced a significant package of new measures in September, listing 70 Iranian individuals and entities including government departments, oil and gas companies, and financial institutions, linked to Iran's nuclear program. Further UK measures in October and November targeted a joint Iranian-St Kitts and Nevis national living in the United Arab Emirates (UAE), alleged to have facilitated hostile activity by the Iranian state overseas. Canada also imposed new autonomous measures in March on Iranian individuals and businesses allegedly helping supply weaponry to Russia, and in December, on four Iranian officials alleged to be involved in repression and torture in the penal system. Meanwhile, Australia did not impose new autonomous measures on Iran; however, it took a rare decision in August to expel the Iranian ambassador, Ahmad Sadeghi, because of 'credible intelligence' that the IRGC was planning arson attacks against Israeli and Jewish targets in Australia.

The Middle East: Syria

One of the most unexpected events of 2024 had been the fall of Syrian dictator Bashar al-Assad in December. Syria then entered a new phase under the transitional leadership of Ahmad al-Sharaa, the leader of the Islamist group Hayat Tahrir al-Sham (HTS).

Despite al-Sharaa's jihadi background, the new president promised an inclusive approach; accordingly, his March 2025 cabinet included representatives from Syria's various ethnic and religious communities. Nonetheless, the situation in Syria remained fragile, with numerous sectarian clashes occurring throughout the year, among the bloodiest of which were the summer confrontations between the Druze (a group following a form of Shia Islam) and Bedouin militias in Suwayda. The situation was complicated further by the ongoing interests of outside powers. Russia, a longtime supporter of the al-Assad regime, developed an uneasy relationship with the new government, which allowed the Russians to maintain their naval and air bases in the country. Turkey became a strong backer of the new government, offering significant aid and funds for reconstruction, though its growing influence in the country alarmed Israel. Israel also voiced concerns about the ongoing dangers of Syrian instability, and at various points mounted airstrikes and cross-border incursions against Syrian forces, which Tel Aviv framed as necessary to protect Israeli security and the safety of Syrian minorities such as the Druze. The new Syria was a policy challenge, too, for Western governments, which had eschewed past engagement with al-Sharaa because of past links to Al Qaeda. Both he and HTS had long been designated as terrorists by the UN, the US, UK and others. Syria also remained under various sanctions imposed by the US, the EU and other Western governments following the start of the Syrian Civil War in 2011.

However, as 2025 progressed, Western governments moved to normalize relations with the new Syrian government. The US revoked its HTS terrorist designation in July, to be followed by the UK and the UN in October. Governments also reviewed their existing economic sanctions, with the US proving boldest of all. On January 6, OFAC issued General License 24, authorizing a wide range of transactions with the Syrian government, military, and other institutions, as well as personal remittances. This was extended to cover a broader range of previously designated targets by General License 25 in May. The most significant development came on June 30, however, when President Trump issued an Executive Order ending the Syrian sanctions regime program, while maintaining measures against members of the former al-Asaad regime, and various other terrorist and criminal groups operating in Syria. The Caesar Act – one of the major legislative underpinnings of US secondary sanctions against Syria – was also repealed in December. Other Western authorities largely followed suit, although somewhat more cautiously. In February, the EU suspended measures on major economic sectors, including energy, transport and finance, and lifted economic sanctions in full in May. The UK made amendments easing its own existing measures in the spring and summer, but did not entirely remove its Syrian sanctions framework. In February (and renewed in August), Canada chose to use a General Permit to allow transactions supporting the humanitarian, stabilization and reconstruction needs of Syria. Australia, by contrast, kept its own Syrian sanctions framework in place, maintaining a case-by-case permitting system for individual transactions.

Prospects for the Middle East in 2026

It is an understatement to say that 2025 was a turbulent year in the Middle East. The significant geopolitical shifts that began in October 2023 continued; Iran and its closest allies encountered one setback after another, leaving Israel militarily dominant across the region, although increasingly diplomatically and politically isolated from potentially sympathetic Arab states, such as Saudi Arabia, and European governments. The major exception, of course, has been the US, where President Trump has shown a permissive attitude towards Israel's use of military force and a readiness to deploy US power to prevent Iran from acquiring a nuclear weapon. President Trump has also reaffirmed his long-standing approach of "maximum pressure" against Iranian sanctions evasion schemes, with the EU, UK, and Canada hardening their own stances in the face of Iran's lack of cooperation with the IAEA.

What, therefore, is 2026 likely to hold in store? The regime in Tehran will likely continue its efforts to consolidate its position at home and mitigate the damage to its interests across the region. Such efforts are likely to include more repression at home, especially as economic protests mount. Beyond its borders, the regime – if it survives – will seek to rebuild the Axis of Resistance, and a focused effort to help Hezbollah in Lebanon seems likely, coupled with attempts to develop ever closer political, economic, and military ties with Russia, China, North Korea, and other countries that reject the Western vision of a 'rules-based international order.' Iran is also likely to accelerate its attempts to quash exiled dissent living overseas and target Israeli and US officials, tourists, and those of Jewish heritage, for violent revenge. The most challenging question to answer, however, is whether Iran will build a nuclear bomb. On balance, the odds seem to be against it, as the regime has continued to state publicly that it does not seek such a bomb and remains willing to negotiate. However, despite the rhetoric, Iran will probably aim to rebuild its nuclear program to a point where it would have the *potential* to build a bomb, if not do so in practice.

This is unlikely to be an unappetizing prospect for the US, Europe, and especially Israel. Given President Trump's unpredictable nature and love of deal-making, there is a reasonable chance that the US might switch from military threats against Iran to offers of indirect negotiations. However, if Trump's past dealings with North Korea and Russia are any guide, those talks are unlikely to result in an agreement.

Consequently, the most probable scenario is a continuation of the US "maximum pressure" campaign against Tehran.

This could escalate to further military action, probably in concert with Israel, triggered either by events in Iran, a major Iran-linked terrorist attack or assassination, or the receipt of intelligence indicating an Iranian rush to develop the bomb. While avoiding military involvement, other Western governments are also likely to toughen their stance on Tehran, implementing new sanctions targeting the regime's evasion efforts, its illicit overseas activities, domestic repression, and support for Russia's war effort in Ukraine.

> *If we want to identify a 'challenger' country on which the US and European approach to sanctions still remains broadly aligned, Iran is the prime example. No Western government wants to see Tehran building a nuclear bomb, and most still see sanctions as an essential tool in preventing that happening. Nonetheless, there's always a chance that President Trump will go his own way in 2026, either through an unexpected diplomatic initiative or further military action.*

Matthew Redhead
Senior Associate Fellow, RUSI

Europe: Russia's war against Ukraine

In February 2025, Russia's full-scale invasion of Ukraine entered its fourth year. Despite dreams of breakthroughs, both military and diplomatic, the war remained attritional, with grindingly slow Russian advances met with stubborn Ukrainian resistance. New levels of uncertainty were introduced into the situation with the return of President Trump, who sought to leverage his claimed personal friendship with President Putin and apply a harsher, more transactional approach to Ukraine in an effort to bring peace.

Ukraine's hard year

For Ukraine, 2025 was another year of 'holding on' as Russia continued to throw men and resources into the battlefields of eastern and southern Ukraine. At ground level, Ukrainian forces suffered several significant defeats. In the spring, Ukraine's military incursion into the Russian Kursk region, which began in August 2024, came to an end, as intense Russian pressure forced the Ukrainians to retreat. The Ukrainian army escaped, according to The Economist, by the "skin of its teeth." In the autumn, the Russians also launched a major offensive to capture the strategically valuable southern Ukrainian city of Pokrovsk, the success of which would open new offensive opportunities for the attackers across the south. In Pokrovsk, as in Kursk and elsewhere on the frontline, the Ukrainian military continued to face one outstanding challenge – not a lack of leadership or determination, but a shortage of manpower.

However tenaciously they fought, the Ukrainians found themselves repeatedly outnumbered by the Russians. Ukraine's civilian population also continued to suffer, as Russia sustained and intensified its drone and missile bombardment of major Ukrainian towns and cities well behind the frontline.

President Zelensky's government also faced numerous political and economic challenges in 2025. Domestically, it faced major demonstrations mid-year when it proposed measures to limit the independence of two anti-corruption agencies – NABU and SAPO. Responding to public pressure, the Ukrainian government reversed these plans. However, the issue of corruption persisted. In November and December, media reports indicated that a long-standing state investigation – Operation Midas – had uncovered a scheme to manipulate contracts of a state-owned nuclear energy company to generate kickbacks for senior officials. Many individuals alleged to be involved were known to be close to President Zelensky, and in late November, his trusted Chief of Staff, Andriy Yermak, resigned after the police raided his home. Beyond domestic affairs, Ukraine also faced a more strained relationship with the US under President Trump. This was most dramatically highlighted for the public by the televised Oval Office meeting between Presidents Trump and Zelensky in February, during which Trump lost his temper and warned Zelensky that he was "gambling with World War Three." Although European governments rallied to Ukraine's side and worked to mend the rift, tensions between the US and Ukraine continued, over the extent of territorial concessions to Russia that Ukraine should make to end the war.

Russia's hybrid campaign

Furthermore, Ukraine was not the only state to face significant external pressure from Russia in 2025. Various European countries faced so-called 'hybrid' or 'greyzone' attacks, which most expert observers assessed to have been sponsored by Russia.

This hybrid campaign involved various strands of covert and sometimes not-so-covert activity, among which the most concerning were acts of sabotage.

Court cases across Europe in 2025 – one of the most notable in the UK – revealed a sustained wave of attempts of Russian-sponsored arson attacks on commercial infrastructure involved in supplying the Ukrainian war effort, as well as acts of strategic vandalism against retail businesses with little connection to the war. More concerning still, 2025 saw Russia increasingly target Europe's Critical National Infrastructure (CNI). In November, for example, a suspected Russian bomb attack on the railway line between Warsaw and Lublin prompted Polish Prime Minister Donald Tusk to describe the situation as "unprecedented." The EU's law enforcement agency, Europol, assessed that Russia was mounting much of this kind of activity using the services of organized crime and petty criminals, as well as a supply of "disposable" migrants from Ukraine and Belarus.

The Russian shadow fleet of commercial vessels was also suspected of involvement in attempts to sever undersea cables in the Baltic Sea, while Nordic governments warned that Russia was preparing similar attacks on cables in the North Atlantic and the Arctic Circle. These maritime activities were also paralleled by Russia's attempts to cause aerial disruptions through sustained GPS jamming of civilian flights across Scandinavia, the Baltic, and eastern Europe, including a September incident that affected a flight carrying Ursula von der Leyen, the President of the European Commission. Russia was also suspected of links to numerous mysterious drone sightings around military, domestic aviation and logistical sites in Belgium, Germany, Norway, Sweden and Denmark in the autumn, which in some cases led to airport closures and canceled flights. In the cyber-sphere, Russia also continued to mount penetrations of Western governmental, commercial, and CNI systems, including a major phishing campaign against Microsoft 365 accounts, discovered in February. It also maintained its position as one of the world's leaders in the dissemination of disinformation. The EU's third Foreign Information Manipulation and Interference (FIMI) report, published in March, pinpointed Russia as the leading malign state actor interfering in European politics and society. Russian media and online disinformation efforts were particularly evident during the Polish presidential election in May and Moldova's parliamentary elections in September.

Overall, Russia's hybrid campaign, while losing momentum in the first months of 2025, accelerated as the year progressed. Analysts concluded that Russia's aim was essentially to disrupt, rather than kill, and to erode European morale and support for Ukraine without triggering escalation; however, the threat that its covert activities might lead to a significant loss of life could not be ruled out. Moreover, the danger remained that the 'real' war in Ukraine itself might spill over into other European countries, as was made evident in September, when mass Russian military drone incursions into Poland and Romania led to the scrambling of military jets and a verbal standoff between Russia and European governments.

Diplomatic runarounds

Diplomatic efforts also provided little relief for Ukraine or its allies in Europe, despite President Trump's expressed desire to bring peace. Trump's bilateral discussions with Putin, mainly by phone, but once in person at a hastily arranged summit in Alaska in August, raised fears among many Western observers that Trump would sell out the Ukrainians in return for improved US-Russia relations. Indeed, Trump repeatedly urged Ukraine to consider territorial concessions to Russia to help progress negotiations, and a proposed US-Russia peace plan, which emerged in November, appeared to favor the aggressor heavily.

Peace did not result in 2025, however, and despite Trump's occasional moments of stated irritation with Putin, Russia remained unwilling to make any significant concessions. Against this backdrop, the EU and European governments sought to maintain the US's engagement and alignment with Ukraine. To address President Trump's complaints about Western states that did not do enough in their own defense, they agreed at the NATO summit in the Hague in June (with some exceptions) to spend 5% of GDP on defense and defense-related spending by 2035. While seeking to keep the US involved in discussions about post-war security guarantees for Ukraine, several European governments also offered to contribute troops to a multinational force deployment to Ukraine – a so-called 'coalition of the willing' – to guarantee any ceasefire. However, this appeared to be a non-starter for Putin, who declared that any such forces in Ukraine would be seen as "legitimate targets." China remained distant from the discussions, despite Putin's demand – rejected by Ukraine – that Beijing be one of the guarantors of any peace deal.

Russia under strain

But Russia did not have things all its own way in 2025. While it made incremental gains, it seemed increasingly vulnerable to long-range Ukrainian missile and drone attacks on its oil industry and strategic aviation. One of Ukraine's most notable successes of the year came in June, when Operation Spider's Web – a sophisticated and highly choreographed drone strike – destroyed or damaged over 20 Russian military aircraft, including around 10 strategic bombers. Russian military casualties also remained extremely high; in November, the UK Ministry of Defense assessed that Russia had sustained approximately 1.14 million casualties – deaths and injuries – since the start of the war, with 332,000 occurring in 2025 alone. Faced with such losses, Russia sought new manpower from abroad. 2024 had already seen the deployment of North Korean troops, which continued into 2025, and they were joined not only by Chinese nationals – apparently without official Chinese government involvement – but also by those of numerous African countries, many of which appeared to have been recruited through social media, through financial incentives and deception.

Cracks began to show, too, in Russia's economy. Towards the end of the year, economic forecasters suggested that Russia was on the verge of entering a recession. Although this did not necessarily mean the Putin regime would be unable to fund the war effort, it suggested that the initial spurt of growth in the first years of the war, driven by military expenditure, was coming to an end. What struck several observers, moreover, were the long-term economic problems now stacking up for Russia, from increased dependency on China to declining Foreign Direct Investment (FDI). Alongside growing economic concerns, there were also some indications of problems within the Putin regime. A familiar series of 'mysterious deaths' of senior officials and oligarchs persisted throughout the year, the most infamous of which was the suicide of transport minister Roman Starovoit, occurring on the same day of his dismissal in July. While possibly explainable by innocent causes, the ongoing high rate of mortality for members of the Putin regime suggested that many of these deaths were suspicious.

Sanctions against Russia

At the start of 2025, Russia faced an extensive multilateral sanctions framework imposed by the US, the EU, the UK, Canada, Australia, and key Asia-Pacific allies. The basic framework had its origin in the Western response to Russia's seizure of Crimea in 2014, but grew massively following Russia's full-scale invasion of Ukraine in February 2022. While each jurisdiction developed its own approach, sanctions were imposed in consultation with partner states and, in some instances, with explicit coordination. The measures focused on five key areas:

- **Russian finances:** Western measures here included freezes on Russian sovereign assets (including $285 billion held by the G7 group of major economies), reduced access to international debt and equity markets, the sanctioning of Russian state financial institutions, including the Central Bank, and significant state-linked commercial banks, as well as the removal of many major financial institutions from the SWIFT cross-border payments messaging system.
- **The Russian energy sector:** The US and its allies developed a complex web of sanctions targeting Russia's oil and gas sectors, from which Russia had long generated significant revenues. These measures included direct import bans on Russian oil, the phasing out of the purchase of Russian gas in Europe (with some exceptions), an Oil Price Cap (OPC) on the sale of Russian oil and related products above a threshold (sitting at $60 per barrel for Russian crude at the start of the year), plus restrictions on investment in many parts of the Russian energy sector.
- **Russia's military or dual-use goods procurement efforts:** Here, Western governments targeted a range of battlefield and dual-use items with potential military value, including advanced technologies such as semiconductors, industrial machinery, and aviation parts for aircraft, missiles, and drones.
- **Russia's logistics and transport sectors:** To undermine Russian sanctions evasion efforts, Western authorities have also imposed restrictions on commercial Russian aviation, road haulage, rail transport, and, most notably, shipping, including port bans and targeted sanctions on Russian firms. Western measures also increasingly focused on the logistical machinery of sanctions evasion through third-country intermediaries and business cut-outs in the Caucasus, the Middle East, Central Asia, and Southeast Asia, as well as Russia's shadow fleet of ageing oil tankers.
- **Senior figures and others linked to the invasion and illicit activities:** Western governments imposed personal sanctions running into the thousands (typically comprising asset freezes and travel bans) against a long list of Russian politicians and officials (including President Putin and Foreign Minister Sergei Lavrov), military and intelligence leaders, business oligarchs, individuals involved in the exploitation of occupied Ukraine, regime propagandists, cyber hackers, and facilitators of sanctions evasion.

In summary, by the start of the year, the Western sanctions regime targeting Russia was among the most detailed and complex applied by Western governments against any state – apart from Iran and North Korea – and one increasingly focused on refinement, implementation, and enforcement within the framework.

2025 developments

The existing sanctions regime against Russia remained largely unchanged by Western authorities and aligned governments in 2025. However, differences in attitude and approach between the US and its allies and partners became increasingly evident as the year progressed.

US measures

Many Western observers worried that the return of President Trump in January would herald a radical new approach to Russian sanctions, with concerns that the President might unilaterally lift sanctions to curry favor with Putin. Indeed, throughout the year, there were signs of a new moderation in the US approach, with the US rejecting proposals in the spring to join the EU, the UK, and others in reducing the oil price, and removing sanctions on Karina Rotenberg, the wife of Russian oligarch Boris Rotenberg, in March. Despite President Trump's shifting attitudes, however, the US did not lift any significant sanctions in 2025. Indeed, at various points, Trump mused about imposing "massive sanctions or massive tariffs, or both" on Russia to encourage flexibility in negotiations. As the year progressed, the US continued to take targeted measures against Russia's energy revenues, its sanctions evasion network, and its financial assets.

US actions against the Russian energy sector began in January, with a final wave of designations from the Biden administration targeting major Russian hydrocarbon firms Gazprom Neft and Surgutneftegas, as well as many of their subsidiaries, and more than 180 Russian oil tankers. In October, reflecting President Trump's frustrations with Russia, OFAC announced significant new designations of the two largest Russian oil firms, Rosneft and Lukoil, explicitly linking them to the need for a ceasefire. The US refused to join in with a G7-wide proposed reduction of the OPC cap, however.

President Trump also showed an increasing willingness to take secondary measures against third countries that continued to buy Russian oil. To the surprise of many Western observers, the US announced an additional 25% tariff on Indian imports into the US (bringing the rate to 50% including existing tariffs), linking the decision to India's ongoing purchase of Russian oil. The Trump administration also expressed sympathy for the bipartisan Sanctioning Russia Act of 2025, which was advancing through Congress. Among its various proposals for stricter measures, it called for tariffs of up to 500% on Russian imports to the US, and, crucially, on imports from countries that continued to buy Russian oil. Nonetheless, President Trump continued to hedge his bets, saying he would only sanction Russia further if NATO allies stopped buying Russian crude oil.

The consistency of the US approach remained somewhat in doubt, however, when, in November, President Trump ordered a one-year exemption for Hungary from US energy sanctions against Russia, with Trump stating that it was "very difficult" for Hungary, led by Trump ally Viktor Orbán, "to get oil and gas from other areas."

The US also continued to target Russian procurement efforts, although with less rigor as the year progressed. In mid-January, it announced a raft of designations targeting regional clearing platforms (RCPs) set up in Russia and China to clear payments supporting sanctioned cross-border trade, as well as the Kyrgyz bank Keremet, which the US alleged was acting as a financial intermediary in Russian sanctions evasion. The Trump administration also focused on using export controls to constrain Russian procurement efforts, with the Department of Commerce's Bureau of Industry and Security (BIS) renewing Temporary Denial Orders (TDOs) against aviation and logistics companies transshipping restricted US goods to Russia. It also announced a far-reaching move on export controls, and one likely to have a significant impact on Russia, issuing an 'Affiliates Rule' in September that extended OFAC's 50% ownership rule to companies subject to export controls. This meant that Russian, Chinese, and other firms affected by US export controls would no longer be able to procure restricted goods through non-listed subsidiaries located outside their home countries. However, in November, the administration suspended the new rule for one year as a concession in ongoing trade negotiations with China.

From Biden to Trump

2025 thus witnessed a notable change in the style and tone of the US response between administrations. Biden had presented Russia as a systemic threat to liberal democratic states and the international order, and had encouraged Western states to work together to degrade Russia's war machine. Trump, by contrast, saw the Ukraine War as an impediment to his desire for better relations with Russia, and one that could be ended through the imposition of tariffs – rather than sanctions – against Russia and its economic enablers – a different approach to the one that the EU, UK, and others continued to follow. Trump, moreover, saw much less need for consistency, taking a fluid approach that privileged US bilateral relationships and diplomatic leverage over Western solidarity.

EU measures

In contrast to the US, the EU largely continued in the same direction of travel set over the previous three years, renewing its existing measures in January and June, and imposing four new, far-reaching packages of sanctions in February, May, July, and October (the 16th, 17th, 18th, and 19th).

These continued to build on the Union's existing sanctions architecture, focusing on the Russian financial sector, energy sales, arms procurement, and the machinery of sanctions evasion:

- **Financial measures:** To tackle Russia's efforts to develop its own payments messaging service, the System for Transfer of Financial Messages (SPFS, based on the English translation of the Russian original), as an alternative to SWIFT, the EU had previously prohibited EU banks outside of Russia from participating in the SPFS system. In 2025, it extended these restrictive measures to several banks based outside Russia, and announced that from January 2026, EU banks would be banned from using *any* other Russian payment messaging service, including "Mir" or the Fast Payments System (SBP). The EU also targeted crypto asset service providers (CASPs) by extending a ban on the provision of EU crypto services to Russian nationals, those living in Russia, and Russian legal entities, and sanctioning the Kyrgyz issuer of the stablecoin A7A5, which was increasingly used in Russian sanctions circumvention efforts.
- **Energy measures:** Europe's ongoing dependence on Russian gas – evident in 2024 – prompted the European Commission to announce a roadmap in May to end the EU's reliance on Russian energy by the end of 2027. The EU also announced a complete ban on transactions involving the Nord Stream 1 and Nord Stream 2 Russia-Germany gas pipelines, as well as a ban on Russian Liquefied Natural Gas (LNG) imports into the EU from January 2027. On oil, the EU followed the US and sanctioned Russian oil major Surgutneftegas in May. The EU also aligned with the majority of G7 members in reducing the oil price cap on the sale of Russian crude oil from $60 to $47.6 per barrel. Its 19th package announced a forthcoming third-country import ban on refined petroleum products made from Russian crude oil, effective from January 2026.
- **Arms procurement measures:** The EU continued to designate businesses it assessed as directly supporting the military and industrial needs of the Russian war effort, many of which were based in third countries in the Middle East, Central Asia, China, India, and Southeast Asia. The Union also tightened export restrictions on dual-use goods and technologies, as well as those linked to defense innovation, including chemical precursors used in riot control agents, and drone control systems.
- **Sanctions evasion measures:** As several of the measures above indicate, the EU also sought to tackle Russia's sanctions evasion machinery, especially at sea. Recognizing the importance of maritime sanctions evasion, the EU introduced a new listing criterion specifically for owners, operators, and enablers of shadow fleet vessels. Throughout the year, the EU added several hundred more tankers to its port-access and maritime services-banned list, bringing the total to over 550 after the 19th package. The EU further expanded its restrictive measures against shipping companies, insurers, reinsurers, traders, brokers, shipbuilders, ports, and maritime registries in third countries that enabled the shadow fleet to operate. Another significant development, announced in the 16th package, was a new due diligence obligation for EU suppliers of sensitive goods to third countries, aimed at reducing the risk that these goods would be transshipped or reexported to Russia.

Beyond these core areas, the EU took other actions specifically intended to undermine Russia's war effort in Ukraine and to target its abuse of human rights in occupied Ukraine. A notable development was the Union's deployment of tariffs on Russian and Belarusian agricultural and fertilizer imports into the EU. Three Russian military entities were also designated in May under the EU's chemical weapons sanctions regime, for their alleged development of riot control agents as a method of warfare. In addition, the EU continued to exercise its designatory powers under its hybrid threats sanctions regime. Designations included individuals and organizations allegedly involved in Foreign Information Manipulation and Interference (FIMI) operations and electronic warfare against civilian air traffic in Eastern and Northern Europe, as well as designations of political and civil society actors in Moldova, alleged to have been engaged in pro-Russian vote-buying and disinformation during election campaigns in 2024. The EU broadcasting licenses for several Russian state-controlled media outlets, which were engaged in systematic disinformation campaigns, were also suspended. Finally, the EU sought to send messages of support to Russia's domestic opposition, sanctioning members of the Russian judiciary involved in the persecution of Russian dissidents, such as Alexei Navalny and Alexei Gorinov.

In sum, the arrival of a new administration and attitude in the US in 2025 led to no significant changes to the EU's Russia sanctions strategy, with the renewal of core restrictions, the addition of four large packages of new measures, and the widening use of specific regimes focused on hybrid threats and human rights abuses. Russian sanctions evasion remained a significant source of concern and action for the EU, and Brussels was willing – albeit in a limited way – to take a page from the Trump playbook, imposing tariffs on Russian and Belarusian agricultural products. Nevertheless, the EU's emulation of the US was limited, and indeed, throughout 2025, the EU showed an increasing willingness to act, with or without the US.

UK measures

The UK followed a similar path to the EU in 2025, renewing existing measures while adding new designations across several major packages. Among the most significant were those announced in February, May, July, September, and October. The UK continued to roll out asset freezes and travel bans against senior figures involved in the

prosecution of the war in Ukraine, including Pavel Fradkov and Vladimir Selin of the Russian Ministry of Defense, Russian extractives businessman Artem Chaika, so-called 'New Kleptocrats' such as Russia's wealthiest man, Roman Trotsenko, and North Korean military leaders involved in the deployment of North Korean forces to Ukraine.

At the same time, the UK pursued sectoral-level responses. Focusing on Russia's energy industry, the UK joined the US in sanctioning oil giants Gazprom Neft and Surgutneftegas in January. Alongside the EU and G7 members, except the US, it supported the reduction of the OPC in July. Targeting Russia's arms procurement efforts, the UK updated its trade restrictions in April to include the export of chemicals used as riot control agents, dual-use electronics and machinery, metals, plastics, as well as technology and software transfers. In addition, the UK pursued a rolling program of designations against those enabling the Russian war effort across the Middle East, the Caucasus, Central Asia, India, China, and Southeast Asia. Designated businesses were alleged to have supplied Russia with a range of sensitive goods and commodities, from machine tools, advanced technology, microelectronics, drone and missile parts to chemicals and explosives.

Many of these firms were owned or controlled by third-country nationals. However, in several cases, such as the China-based Shenzhen Blue Hat International Trade Ltd., the targets, though ostensibly non-Russian firms, were owned by Russian nationals (in this instance, Elena Malitckaia and Alexey Malitskiy).

The UK also joined wider efforts to degrade Russia's sanctions evasion machinery, especially its shadow fleet. Like the EU, the UK targeted multiple vessels throughout the year, with over 500 listed by November. The UK also sought to target the ecosystem of Russian enablers, intermediaries, and buyers behind the fleet. Notable examples included John Michael Ormerod, a British national alleged to procure vessels for the fleet; Intershipping Services, responsible for registering tankers under the Gabonese "flag of convenience"; Orion Star Group, which helped crew and manage vessels; and financial institutions such as the St Petersburg Currency Exchange and the Russian Deposit Insurance Agency, which provided insurance services for vessels. Furthermore, the UK took several steps to counter Russia's financial sanctions evasion machinery in Central Asia. In February, this included the UK joining the US in listing Keremet Bank. In August, a network of other Kyrgyz-based financial entities and individuals, including Capital Bank, its director, Kantemir Chalbayev, and cryptocurrency exchanges Grinex and Meer, was targeted, with the key infrastructure being the A7A5 stablecoin.

The UK also aligned with the EU's approach by extending its sanctions against those involved in oppressive activities in occupied Ukraine, including attempts to erase Ukrainian culture. In September, the UK designated the Akhmat Kadyrov Foundation, its president, Aymani Nesievna Kadyrova (mother of Putin's Chechen ally Ramzan Kadyrov), Valery Maiorov, the Head of 'Teenage Programs Center', and Anastasia Pavlovna Akkuratova, of the Russian Ministry of Education, for their involvement in the deportation and indoctrination of Ukrainian youth. The UK targeted Russian hybrid activities too, including Russian military intelligence (the GRU), its cyber activities, and its attempts to map undersea cables in the seas around the UK. The UK's concerns were not limited to hybrid threats to the UK alone; moreover, in April, it sanctioned several senior figures in Evrazia, a Russian non-profit operating in Moldova, linked to the UK-designated oligarch and fugitive Ilan Shor. According to the UK, Shor had used Evrazia to funnel around $15 million in bribes to voters in Moldova's 2024 EU membership referendum to try – unsuccessfully – to secure a no vote.

Canada and Australia

Further afield, both Canada and Australia – both of which have been less directly affected by the war in Ukraine than those in Europe – continued to align with the EU and UK's approach to Russia, and both supported the decision to reduce the OPC in the summer. Canada also imposed new import and export prohibitions on sensitive items involved in the production of chemical and biological weapons, machine goods, and dual-use advanced technologies. It announced further designations of Russian officials and businesspeople who had profited from the war, numerous shadow fleet vessels, third-country intermediaries and enablers of Russian arms procurement efforts, including those in support of drone production, and joined the EU and UK in targeting Russian hybrid interference overseas, including individuals associated with Ilan Shor's Russian-backed efforts to destabilize Moldovan democracy. Australia also expanded its sanctions regime against Russia in 2025, targeting individuals involved in the administration, exploitation, and repression of Russian-occupied territories in eastern and southern Ukraine, senior Russian officials, businesspeople, media figures, and the supply of drone parts and components.

Most notably, Australia also imposed its first sanctions on the shadow fleet, listing 60 vessels in June, and a further 95 in September.

Targeting Russia's partners and proxies

Since the start of Russia's full-scale invasion in 2022, Western governments have imposed many of the same or similar measures against Russia's neighbor and ally, Belarus, led by President Alexander Lukashenko. In 2025, sanctions activity against the regime tracked the approach they were already taking towards Russia. New EU sanctions against Belarus arrived in parallel with the latest Russia packages, essentially matching trade-related measures, transport restrictions, technology and software transfer, and crypto-focused controls imposed on Russia. The EU also included Belarus in its new tariff regime on agricultural exports and fertilizers – a significant source of income for Belarus. The UK and Canada added additional designations of senior Belarusian officials, including the Chairman of the Belarusian Central Election Commission, after what they described as a "sham" presidential election returned Lukashenko to power in January. Both countries also applied new measures against individuals allegedly involved in human rights abuses. Australia, by contrast, made no significant additions to its Belarusian sanctions framework, and in the US, a slight and partial reversal began. While retaining most of its existing measures, the US started a process of sanctions relief, with OFAC issuing General License 11 in September and General License 12 in November, easing restrictions on transactions with the Belarusian airline Belavia and several specific aircraft. The BIS supplemented these changes by authorizing Belavia flights and maintenance that had previously been restricted.

A further country of increasing concern to several Western governments in 2025 was Georgia, following the allegedly fraudulent victory of the pro-Russian Georgian Dream party in the October 2024 parliamentary elections. In January, the EU partially suspended its visa facilitation scheme for Georgian diplomats and officials in response, but despite intense pressure from the European Parliament, its Council did not agree on any measures against Bidzina Ivanishvili, the leader of Georgian Dream (designated by the US in December 2024), or other Georgian figures. The UK did take several actions, however, targeting the corrupt 'Judicial Clan' linked to Georgian Dream in April, and alleged Georgian enablers of Russian sanctions evasion, including media magnate Levan Vasadze, in September.

Russian headaches: Evasion, third-country compliance, and state assets

Despite the persistence and extension of Western economic and financial measures against Russia, ongoing vulnerabilities and weaknesses remained apparent. Sanctioning authorities sought to emphasize the success of sanctions; in June, the UK government estimated that as of February 2025, Western actions had deprived the Russian state of $450 billion, of which $154 billion was lost tax revenue from Russian oil sales. Nonetheless, there was no obvious evidence that these losses had had any substantial effect on Russia's will to keep fighting or on hindering its war effort.

Available evidence also suggested that Western sanctions continued to face resourceful Russian sanctions evasion efforts. In June, an analysis by the UK broadcaster Sky indicated that over the previous nine months, the flow of dual-use goods to Russia's neighbors had risen by an average of 9%, standing 111% above pre-invasion levels. Sky also found similar patterns in the United Arab Emirates (UAE) and Turkey, both of which have featured as popular transshipment hubs. The prominent role that companies and individuals in third countries played in Russian sanctions evasion schemes further highlighted the stubborn problem of non-Western governments' noncompliance with the West's approach. China, India, and several major middle powers across the Global South continued to assert that globally relevant sanctions could be applied only by the UNSC, and that autonomous measures issued by the US, EU and others had no extra-territorial effect. This statement of principle also went hand in hand with keen self-interest. Restrictions on the sale and purchase of Russian oil caused issues for countries such as India, which remained heavily dependent on foreign energy supplies, and annoyance about the secondary targeting of their private-sector firms engaged in trade with Russian businesses. Several of these 'neutral' governments further asked why a conflict in Eastern Europe should have such a broad impact on the global economy's economic and financial stability.

But not all the West's problems arose from Russian ingenuity or the divergent interests of non-Western powers. Issues with the domestic Western implementation of Russia sanctions remained apparent, with the EU itself noting that Russian crude continued to be sold into Europe from third countries, mixed with, and/or re-badged as, product originating from other countries. Western disagreements about how to apply further economic and financial pressure on Russia persisted as well.

Western disagreements about how to apply further economic and financial pressure on Russia persisted as well. From the start of the war, there had been an ongoing debate about seizing the $285 billion in immobilized Russian state assets sitting in Western institutions (most of which were held by Euroclear, a securities depository located in Belgium) to fund the Ukrainian war effort and postwar Ukrainian reconstruction (referred to as going 'from freeze to seize'). In 2024, some progress was made, with interest from sovereign Russian funds frozen in the EU transferred to the Ukrainians in July. However, deeper questions about the use of the underlying funds remained, with officials debating the legal implications of confiscation, the risks of market destabilization, the potential for Russian retaliation, and the potentially degrading effects on international financial norms.
The European Commission developed a plan in 2025 to work around legal difficulties and other risks, suggesting instead that rather than seizing Russian funds outright, EU governments could use Russian funds as collateral for a loan to Ukraine. Despite its fluid stance on Ukraine, the US saw merit in the approach. But while the EU Council showed support for the concept in principle in October, at its December meeting, it decided instead to make a €90 billion loan (around USD 105 billion) to Ukraine unconnected to frozen Russian assets. This outcome was caused by national disagreements and the anxieties of some governments about how the Russian government might react to the use of their assets, however indirectly, with Belgium seeking explicit guarantees and protection against future Russian financial claims.

Prospects for Russia and Ukraine in 2026

Scenarios for the development of Western sanctions against Russia in 2026 depend on the likely state of the battlefield, potential political developments in Russia and Ukraine, and ongoing US diplomatic efforts to bring the war to a conclusion. Given the variety of imponderables involved, therefore, any predictions should be treated with extreme caution. Based on the current situation, three broad possibilities seem plausible: first, that the US will manage to impose and sustain a peace deal that proves bearable to Ukraine and acceptable to Russia; second, that such efforts fail and the war grinds on throughout 2026 following the same attritional pattern as previous years; and third, one side or another achieves victory, whether as the result of a battlefield collapse by one side or another, dramatic domestic political changes, or the loss of support from a major outside backer (i.e., the US or China).

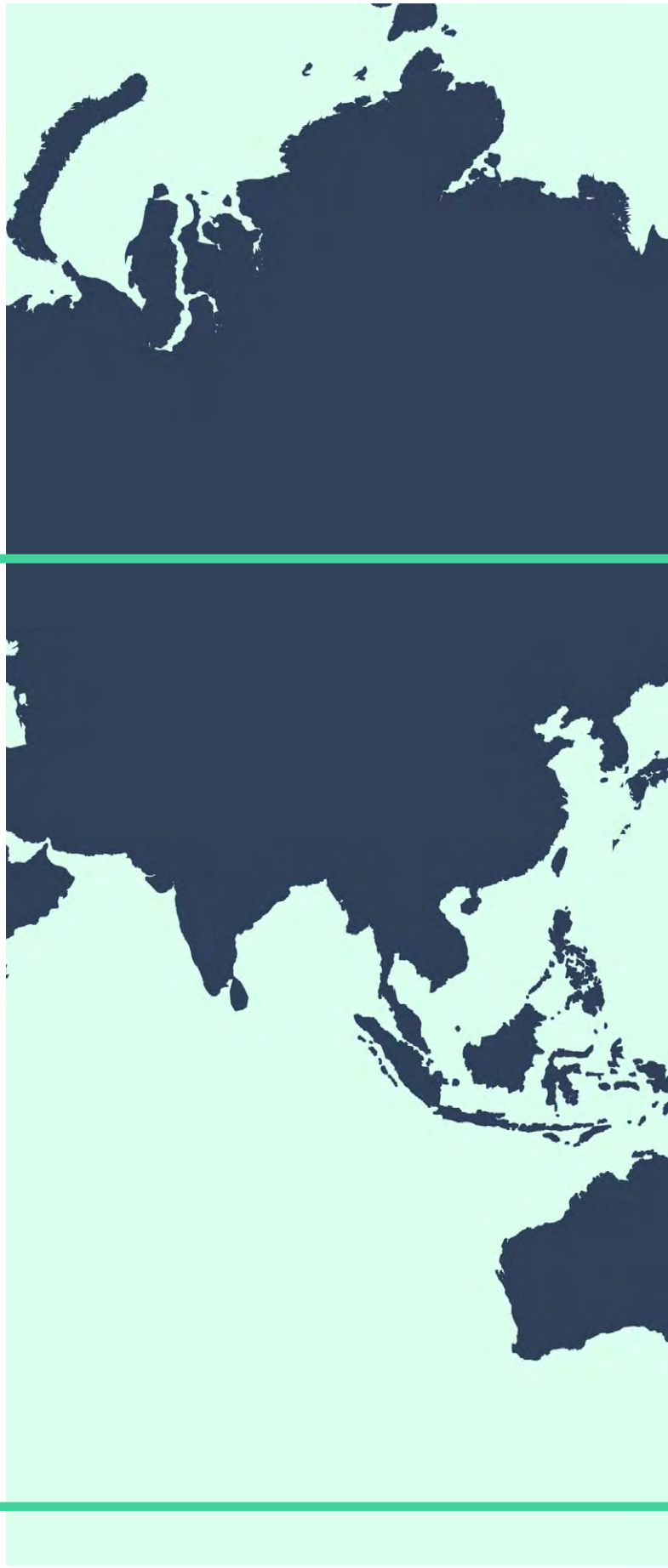
In the first instance, US sanctions against Russia will likely be rolled back, although probably with a proviso allowing their reimposition if Russia breaches any deal, largely to appease the US's allies and the anti-Russia Republicans in the US Senate. The EU, UK, and others are likely to be more circumspect about removing their most significant sanctions quickly, however, and will wait to see if any agreement holds. In the second scenario, the current approaches of the US, EU, and others will remain broadly the same: the US maintaining but not extending its current measures, other Western authorities continuing to build on the current framework, while also progressing with plans to provide a collateralized loan to Ukraine. It is also possible, though unlikely, that President Trump will make a dramatic move to pressure Russia by utilizing the provisions of the Sanctioning Russia Act (if ever passed – at the end of the year it remained "pending legislation") to impose new sanctions and tariffs on Russia, as well as tariffs on third countries that import Russian oil. In the final scenario – a decisive end to the war – would also likely encourage the US to quickly roll back its own sanctions on Russia, in an effort to draw a line under the conflict. Once again, other Western allies – especially in Europe – are likely to be more circumspect in their approach, particularly in the event of a Russian victory. Indeed, such an outcome might lead to a significant divergence between the US and its erstwhile partners, with the EU, UK, and Canada seeing the need to continue supporting Ukraine and to contain future Russian aggression through ongoing sanctions.

The question, therefore, is which of these scenarios is likeliest to evolve. On balance, it remains the second scenario – an attritional conflict, with both sides refusing to concede defeat or make necessary concessions. A decisive victory for either side seems the least probable outcome, but an imposed peace, forced on Ukraine by an impatient US, is increasingly possible. To make that happen, and to make it stick, however, President Putin will also have to prove willing: something which can never be taken for granted.

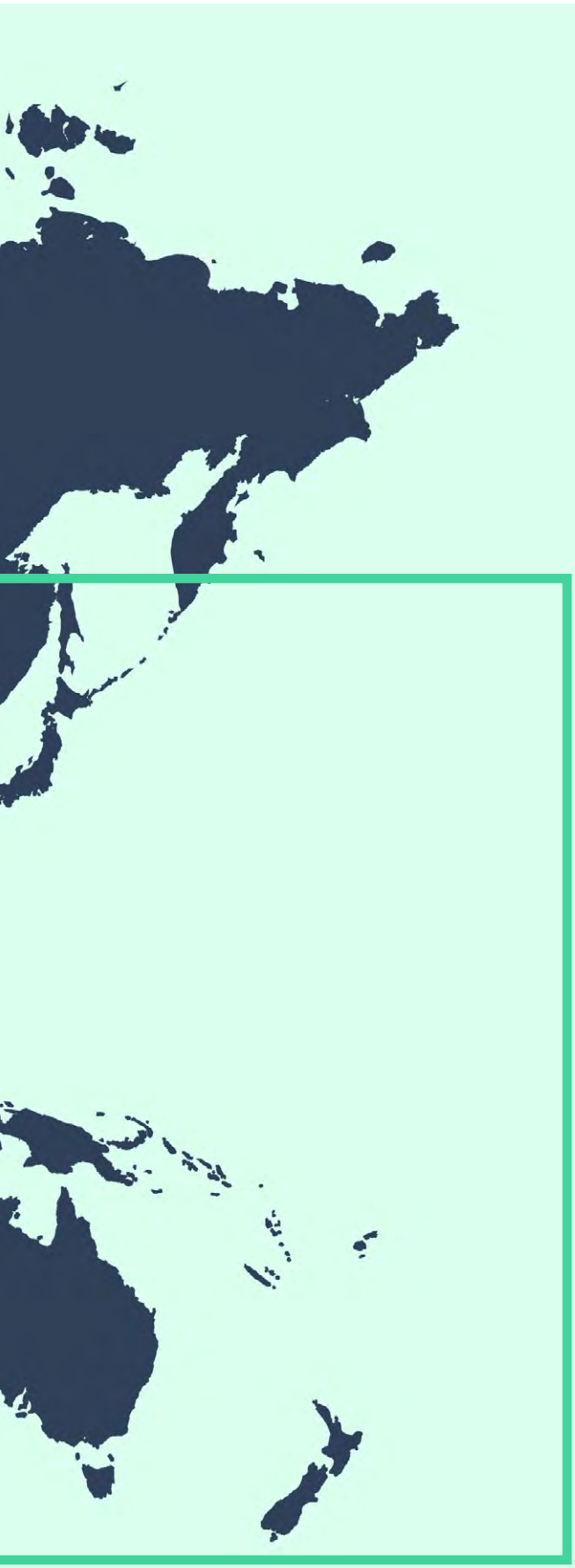
Regional review

Asia Pacific

In previous years, our State of Financial Crime report has highlighted several areas in the Asia Pacific as major global hotspots and a focus of both multilateral and national sanctions activity. In 2025, by contrast, the range of new sanctions against primary targets in the region was both relatively limited and narrowly focused.



During 2025, North Korea continued to behave provocatively, conducting numerous short and medium-range missile tests in the seas around the Korean peninsula,



while seeking to develop an Intercontinental Ballistic Missile (ICBM) that would have the range to strike the US homeland. Border incidents with South Korea increased throughout the year, with several reports emerging of North Korean troops crossing the land-based Military Demarcation Line (MDL). Pyongyang's campaign of cybercrime continued at pace, too, aided by North Korea's clandestine program to deploy hackers remotely in cyber roles in the West, and to use fake job opportunities to trick overseas software developers into downloading malware. In February, the FBI announced that North Korean cyber hackers had been behind the theft of $1.5 billion of cryptocurrency from the ByBit cryptocurrency exchange, the largest single case in crypto history so far. By October, the blockchain analytics firm Elliptic estimated that North Korea had already accumulated over $2 billion in crypto in 2025, suggesting it was on track for its biggest annual haul ever. Finally, North Korea continued to support Russia's war in Ukraine with munitions and troops, despite suffering heavy losses.

In response to Pyongyang's behaviour, UNSC measures targeting the regime's nuclear and ballistic missile program remained in place; however, with both Russia and China intransigent about the need for additional action, no new UNSC resolutions were passed. The UNSC's North Korea Panel of Experts, tasked with monitoring the implementation of UN sanctions on the country, was also not revived after the Russian veto of its mandate renewal in March 2024. As a result, a group of 11 countries (Australia, Canada, France, Germany, Italy, Japan, the Netherlands, New Zealand, South Korea, the UK and the USA) came together to form their own Multilateral Sanctions Monitoring Team (MSMT), which held its first steering committee meeting in February 2025, and issued its first statement in May.

Alongside the development of the MSMT, several states took several focused actions under their own autonomous regimes. Their most prominent target was North Korean cybercrime, with the US taking the lead by designating networks of North Korean state-linked cyber actors and state-linked entities, intermediary firms, and facilitators in Russia and China in July and August, and North Korean bankers and state-owned enterprises involved in laundering funds from these and other illicit schemes in November. Australia also imposed sanctions on several North Korean state-linked cyber actors, including the infamous 'Lazarus Group' in November, while both the UK and Canada issued advisory guidance to the private sector on the risk from North Korean remote IT workers.

In addition, North Korean arms transfers to Russia and Myanmar raised ongoing concern. In the latter case, the US imposed new measures in September, targeting North Korean facilitators, the Burma-based Royal Shune Lei Company, and its key staff, for their involvement in organizing weapons sales from the Korea Mining Development Trading Corporation (KOMID) to Myanmar's air force. Nonetheless, the scale and scope of Western sanctions activity against North Korea remained relatively limited in 2025, with governments distracted by events in the Middle East and Europe. Moreover, many suspected that the US's relative lack of action reflected President Trump's ongoing desire for a new summit with President Kim Jong-Un, the prospect of which had begun to rise by the end of the year.

Beyond North Korea, Western sanctions in the Asia-Pacific region, specifically targeting state actors (rather than non-state criminal groups involved in scams and human trafficking discussed shortly), were also relatively limited in 2025. Various Western measures against the military regime in Myanmar remained in place – the EU, for example, renewed its existing measures for another year in April – but in most cases, no new designations were brought against the Junta. The exception was Canada, which in March designated 13 senior regime officials and three entities.

Despite fears in Beijing that the return of President Trump would herald a new wave of China-focused sanctions, the number of US designations targeting Chinese state-linked actors was limited in 2025. Two of the most noteworthy US moves of the year – against commercial firms being used as proxies by Chinese state cyber-hacking units, 'Flax Typhoon' and 'Salt Typhoon' – came in January, before the inauguration of the new President. The US designation of six Hong Kong officials and law enforcement officers in March for the persecution of pro-democracy activists in the territory was a lonely addition to existing US measures on Chinese human rights abuses: an area where there had been substantial designatory activity during the first Trump administration.

Another area of perhaps unexpected change to the US approach towards China came in the realm of export controls. By the end of his term in office, President Biden had put in place a range of stringent controls designed to limit China's access to advanced microchips, microelectronics, quantum computing, and AI technologies that might be used for military purposes.

These measures included the Outbound Investment Security Investment Program, which prohibited or restricted US investments in Chinese technology research, and came into effect at the start of January 2025, and the 'AI Diffusion Rule,' introduced in mid-January, which aimed at limiting the export of advanced US AI models to countries of concern, such as China, Russia, Iran and North Korea.

The new Trump administration did not entirely repudiate the Biden approach. However, it made several significant alterations to the model, loosening in some respects and tightening in others. The loosening included setting aside the AI Diffusion Rule in May, citing concerns about its effect on US innovation, and concluding an arrangement with US tech firms Nvidia and AMD in August that would see the US government receive 15% of the firms' revenues from sales of advanced chips to China, in return for the receipt of export licenses. At the same time, the administration added new Chinese entities to the Department of Commerce's Entity List in March and removed export rule exemptions for several South Korean- and Taiwanese-owned China-based chip fabrication plants in September.

Overall, the impression emerged that Trump sought to both constrain Chinese technological development and benefit financially from it.

The Chinese did not respond positively to the new US approach, which brought forward new export controls on rare earths and magnets essential to the US defense supply chain.

If the US approach to sanctions and export controls on China underwent refinement and modulation in 2025 – if not a significant extension – there *was* a notable shift in US tariff policy towards Beijing. Of course, China was far from being alone in facing President Trump's predilection for using trade as a means of persuasion, with numerous others, including many US allies, facing new duties. Nevertheless, China was among the countries that faced the most draconian measures. In less than three months, from February to April, cumulative US tariffs on China rocketed from 10% to 145%, before falling back to a negotiated "truce rate" of 30% in May, and then to a new "temporary" rate of 20% in October (composed of the basic 10% reciprocal tariff, and 10% a reduced fentanyl tariff). These tariffs were not uniquely linked to US national security concerns in the administration's rhetoric; economic issues, such as a perceived Chinese boycott of US agricultural goods, featured strongly. However, there was an undeniable and explicit security dimension to the President's actions, with China's approach to the supply of fentanyl precursors to Latin American cartels, and its attempts to restrict US access to rare earths, cited among the reasons for the imposition of tariffs.

Beyond the US, the EU, UK, Canada, Australia, and other countries took a relatively circumspect approach to China, taking little targeted action against Chinese state actors. Instead, as noted in previous sections, these states increasingly targeted *private* Chinese businesses and businesspeople whom they implicated in Russian and Iranian sanctions. While the EU and UK did not explicitly point the finger at the Chinese government in these instances, they highlighted and targeted Chinese companies, along with other third-country private-sector enablers, in various sanctions packages across the year.

The Americas

US sanctions-related activity in the Americas throughout 2025 focused on various Latin American cartels (discussed in more detail in the Thematic Review below). Still, government actors were also targeted, mainly in the context of the Trump administration's anti-narcotics campaign. In October, the Colombian President, Gustavo Petro, along with several family members and associates, was designated for his government's failure to tackle cocaine production in the country.

However, the central state of concern to the US was Venezuela, led by President Nicolas Maduro.

In recent years, the Biden administration had sought to improve its relations with Maduro's leftist-nationalist regime, offering limited relief from US oil sanctions in the hope of encouraging a fair presidential election in July 2024. However, as it became clear in the spring of 2024 that Maduro intended to remain in power, President Biden reimposed sanctions. After the election on July 28, amid evidence of widespread vote-rigging, Maduro claimed victory; on January 10, 2025, after a period of violent domestic repression, he was sworn into office for a third term as president.

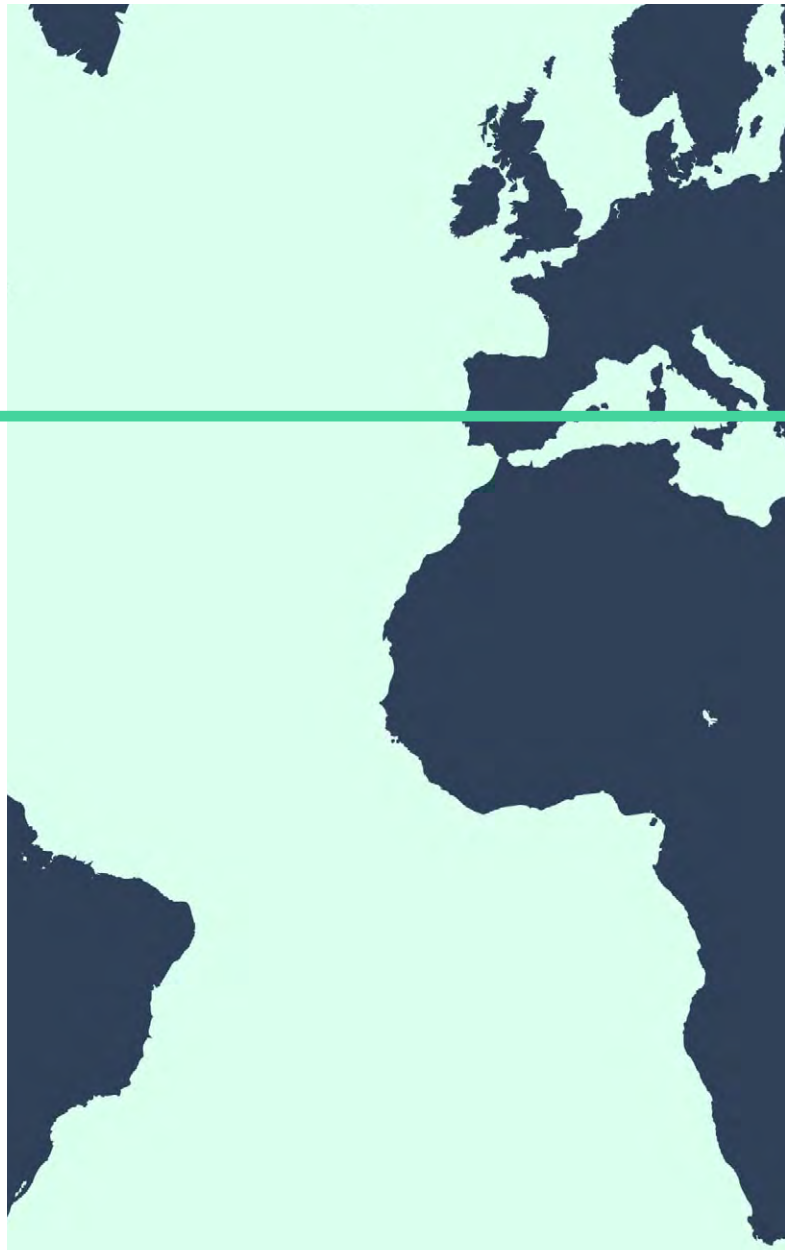
The approach of the outgoing Biden administration to Maduro's re-inauguration was to designate eight senior Venezuelan officials and business figures, including the presidents of the country's state-owned oil company, PdVSA, and state-owned airline, CONVIASA. The Biden administration also increased an existing reward for information leading to Maduro's arrest on narcotics charges from $15 million to $25 million (other rewards

for similar information on other Venezuelan officials were also increased). Canada, the EU, and the UK imposed their own measures on senior Venezuelan military officers, election officials, and members of the judiciary in parallel. In March, Canada added eight more individual designations. But with the return of President Trump, the overall tone of the US's response hardened, with the new administration announcing a 25% tariff on countries that bought Venezuelan oil in March. The President also took a harsh rhetorical tone towards Maduro, increasingly framing him and his regime as "narco-terrorist," and explicitly naming him and his associates as the leadership of the Venezuelan cartel, the 'Cartel de los Soles.'

During late spring and early summer, there were indications of engagement between the two sides – in July, Chevron was reported to have received a renewed, but limited, license to operate in Venezuela – but by September, the character of the US approach began to shift from the economic to the military realm, as it undertook successive air attacks on civilian vessels in the Caribbean, which the administration claimed were involved in drug-running. Although these attacks were not explicitly presented as attacks on the Maduro regime, most of the strikes targeted ships leaving Venezuela. From late August, a massive US naval buildup – including the deployment of an aircraft carrier – began in the Caribbean. Despite the Trump administration's claims that the US maritime presence was intended to support existing anti-narcotics actions, it was evident to expert observers that the deployment was designed to put extreme pressure on Maduro, who US officials continued to link to "narco-terrorism." This link was made explicit on November 16, when Secretary of State Marco Rubio announced the designation of the Venezuelan Cartel de los Soles as a Foreign Terrorist Organization (FTO), naming Maduro as its leader, following the group's designation as a Specially Designated Global Terrorist in July. As the US military buildup continued, the US let it be known that covert operations against the Maduro regime had been authorized. In November, Trump announced that Venezuelan airspace was now "closed" and in December, the US began a naval blockade of tankers carrying Venezuelan oil, seizing and pursuing several. As the year ended, everything pointed towards further US action, an expectation that was realized on January 3 2026, when US forces kidnapped Maduro from Caracas, and took him to New York to stand trial. Maduro was succeeded by his deputy, Vice President, Delcy Rodriguez, who, while stressing Venezuela's ongoing independence, sought to work with US Secretary of State Mario Rubio. However, with President Trump suggesting that the US would 'run' Venezuela (and its oil industry), the long term prospects for the country remained highly uncertain.

Africa

In Africa, international attention in 2025 was most firmly focused on Sudan, where a brutal civil conflict between the Sudanese Armed Forces (SAF), the official national military, and the paramilitary group the Rapid Support Forces (RSF), continued. By the late summer, estimates suggested that around 400,000 people had been killed, mostly civilians, since the start of the conflict in April 2023.



A key moment in the year came when the RSF captured El Fasher, a SAF stronghold in Darfur, after a year-and-a-half-long siege.

The RSF marked their victory with mass executions and organized sexual violence, triggering a stream of refugees to neighboring towns across southern and western Sudan.

The US responded by targeting senior commanders in the warring factions. In January, the US designated both Mohamed Hamdan Dagalo ('Hemedti'), the leader of the RSF, and General Abdel Fattah al-Burhan, commander of the SAF, citing their responsibility for atrocities against civilians and obstruction of international humanitarian access, as well as businesses and facilitators involved in the groups' logistical and financial support networks. In September, the US followed up with designations of Islamist leader Gebreil Ibrahim Mohamed Fediel, Sudan's

Finance Minister and the chair of the Justice and Equality Movement (JEM), as well as the Al-Baraa Bin Malik Brigade (BBMB), an Islamist militia which the US alleged has close military ties to Iran. Alongside the US, Canada made two rounds of Sudan-related designations in February and March, also targeting leading figures in the RSF and SAF, those allegedly implicated in weapons procurement efforts and the use of sexual violence as a weapon of war. In addition, the EU slightly expanded its Sudan designation list in July, adding two new individuals and entities. It also renewed its existing sanctions regime against SAF and RSF figures and affiliates in September.

Further south on the continent, the long-running conflict in the Democratic Republic of Congo (DRC) between the Congolese national army (the FARDC), the Rwanda-backed March 23 Movement (M23), the Islamist Allied Democratic Forces (ADF), multiple other militias, as well as the armed forces of Burundi and Uganda, persisted. Early in 2025, M23 enjoyed several military successes, taking Goma in January and then advancing across the North and South Kivu provinces, while the ADF conducted attacks against civilians, including an attack on a hospital in the autumn.

The US responded to the situation in February by designating James Kabarebe, Rwanda's Minister of State for Regional Integration (and a leading supporter of M23), and Lawrence Kanyuka Kingston, a senior member of M23, as well as two of Kanyuka's companies registered in the UK and France. In August, this was followed by the designation of the Coalition des Patriotes Résistants Congolais-Force de Frappe (PARECO-FF), its illicit mineral mining activities in Rubaya province, and the Hong Kong-based businesses linked to it. But the US's main efforts in DRC in 2025 were diplomatic. In June, the US brokered an agreement between the DRC and Rwanda to end the war, with the former ending its support for an anti-government militia in Rwanda, and the latter promising to remove all its troops from the DRC. The agreement was underpinned by a further economic agreement between the two governments signed in November, and the formal signing of the accords by the countries' two presidents in Washington, DC, in December. In November, M23, the leading armed rebel group, also signed a peace accord with the government of the DRC. Nevertheless, concerns remained about the sustainability of the agreements, as both sides continued to move forces and reinforce their positions in eastern DRC.

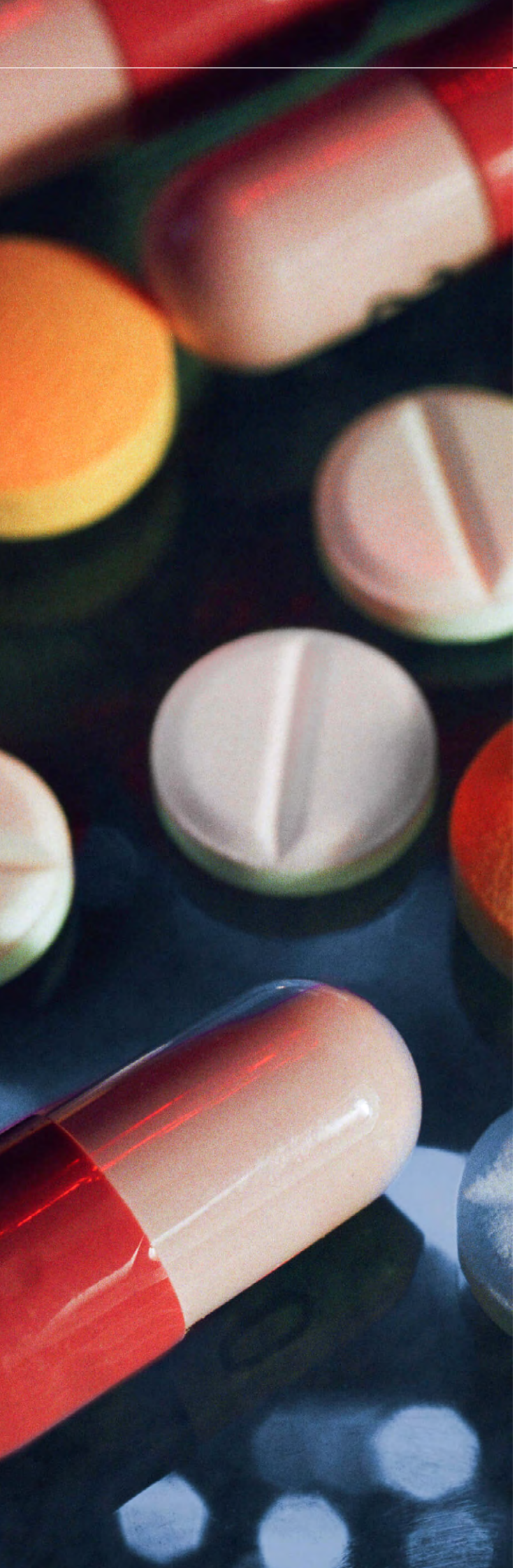
Thematic review

The US and "Narco-Terrorism"

A central pivot in US strategy in 2025 was to focus its most concerted sanctions-related action on organized crime groups (OCGs) operating in Latin America and the Caribbean. On his first day in office, President Trump signed an Executive Order allowing the designation of major drug cartels – formerly seen only as transnational criminal organizations (TCOs) – as foreign terrorist organizations (FTOs) and specially designated global terrorists (SDGTs). One month later, the Department of State used its new powers to specifically designate six Mexican groups (the Sinaloa Cartel, Cartel de Jalisco Nueva Generación (CJNG), Carteles Unidos (United Cartels), Cartel del Noreste (a successor faction to Los Zetas), Cartel del Golfo (Gulf Cartel) and La Nueva Familia Michoacana (LNFM), one Venezuelan (Tren de Aragua), and one El Salvadorean/ Honduran (Mara Salvatrucha (MS13) as national security threats to the US. In May, the Department of State added two Haitian gangs, the Viv Ansanm coalition and Gran Grif, to this list. Central American gang Barrio 18 was designated FTO/SDGT in September, and as previously noted, the Cartel de los Soles (Cartel of the Suns) in Venezuela was designated an SDGT in July and an FTO in November. In December, the Colombian group, Clan del Golfo, was also added to the FTO/SDGT list.

Applying FTO and SDGT designations significantly broadened the US's policy toolkit. Firstly, making cartels FTOs made any of their members inadmissible to or removable from the US, allowing the federal government to apply the non-criminal standard of proof used by immigration authorities. The FTO designation also allowed the US to prosecute any individual who provided practical support – funding, transport, protection, etc. – to a designated group under federal terrorism statutes, carrying a penalty of up to 20 years in prison. Separately, the SDGT label also allowed the US to expand sanctions designations to a broader range of targets deemed to be providing "material support," including foreign financial institutions, real estate brokers, and accountants. US authorities moved quickly to use these powers throughout the year, with the primary targets being:

- **The Sinaloa Cartel:** Despite the US's arrest and incarceration of several of its major leaders over the last decade (the most famous being Joaquín 'El Chapo' Guzmán), the Sinaloa Cartel remained a major supplier of illegal fentanyl into the US market. In 2025, the US focused on its two powerful (and warring) factions – Los Chapitos, led by El Chapo's children and key lieutenants, and Los Mayos, led by Juan Jose Ponce Felix ('El Ruso'). US designations included the factions themselves, individual faction leaders, money launderers and linked gambling syndicates, as well as firms supplying them with precursor chemicals and laboratory equipment.
- **CJNG:** The group, led by Rubén Oseguera Cervantes ("El Mencho"), is reputed to be one of the most violent Mexican cartels. In 2025, US designations targeted its senior leadership (including El Mencho), a network in Tamaulipas running an oil-smuggling and fuel-theft operation described as a "cash cow" for the group, and a further network of individuals and companies linked to timeshare fraud in the holiday destination of Puerto Vallarta.
- **LNFM:** LNFM, co-led by brothers Johnny 'El Pez' Hurtado Olascoaga and José Alfredo 'El Fresa' Hurtado Olascoaga, is a cartel with diverse interests in drugs, illegal mining and extortion. On April 15, the US designated both brothers and several other senior leaders. On the same day, the group's leaders and an Atlanta-based money launderer were indicted by the Department of Justice for conspiracy to manufacture and supply a variety of illegal narcotics.
- **Cartel del Noreste:** A cartel that arose from the fragmentation of the 'Los Zetas' cartel in the 2010s is known for its tight control of the US-Mexico border region. In May, the US designated two senior group leaders involved in cross-border drugs and weapons smuggling, and for their alleged involvement in a 2022 attack on the US Consulate in Nuevo Laredo. Three further senior cartel figures were sanctioned in August.



- **Tren de Aragua:** US officials highlighted this Venezuelan group as a rising threat in the Caribbean throughout 2025. In June, the US designated Giovanni Vicente Mosquera Serrano, a fugitive senior leader of the group who has overseen much of its operations in Colombia. The action was taken in parallel with his addition to the FBI Ten Most Wanted List. It was followed, in July, by the designation of the group's leader, Hector Rusthenford Guerrero Flores ('Niño Guerrero'), and other group leaders and associates. In December, the US also targeted a number of entities and individuals allegedly involved in the cartel's money laundering operations.

Alongside the new use of the FTO/SDGT designation against major cartels, the Trump administration continued to apply pre-existing criminal legislation (typically the Kingpin Act of 1999) to target illicit narcotics networks not deemed to be involved in terrorism. In 2025, these designations included:

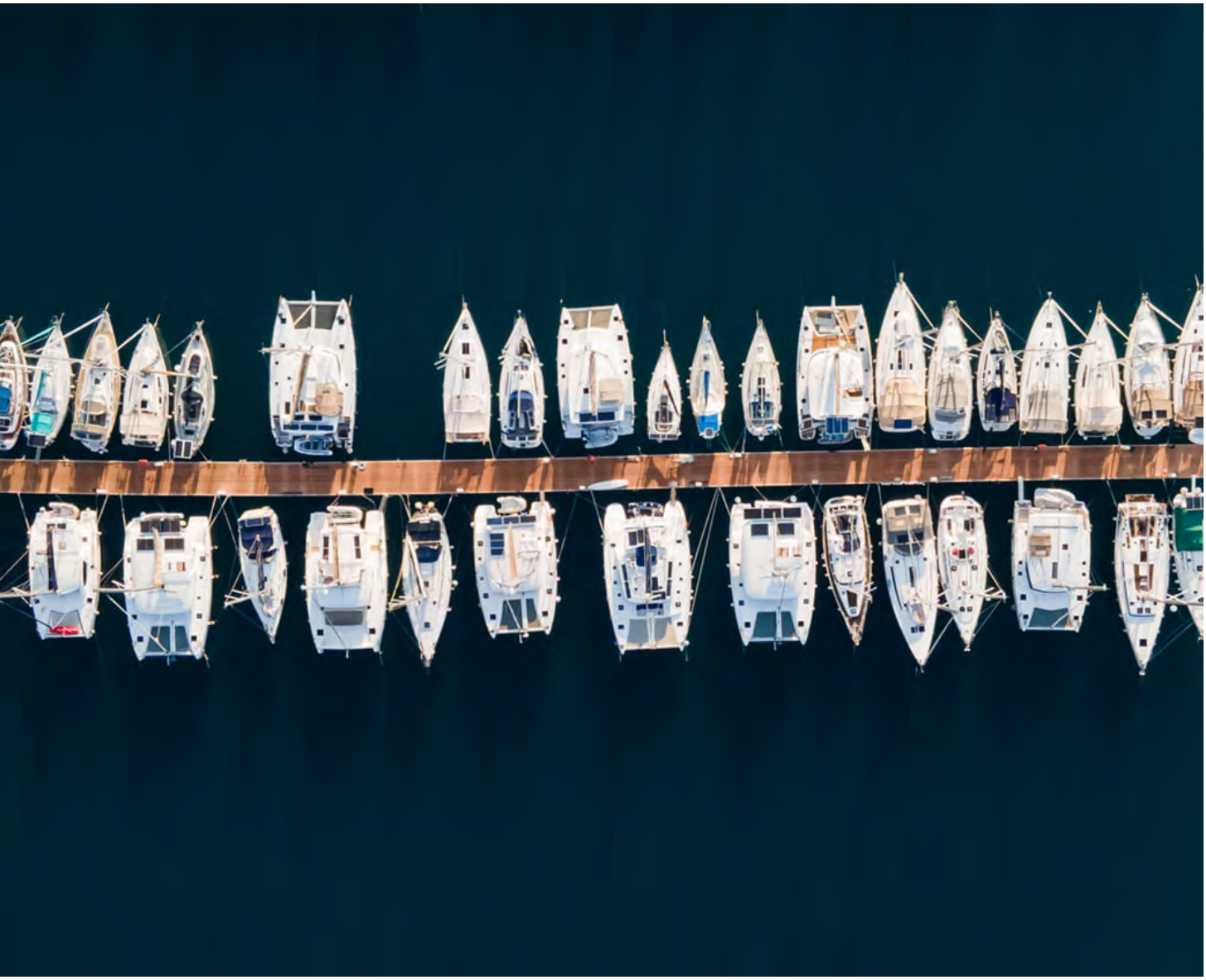
- Jesús Alfredo Beltrán Guzmán, a leader of the Beltrán Leyva Organization (BLO), implicated in the trafficking of fentanyl and other drugs into the US.
- Guyanese nationals (including a corrupt law enforcement officer) and Colombians for transporting cocaine by boats, narco-subs, and aircraft from Colombia and Venezuela via Guyana and Suriname to the US, Europe, and the Caribbean.
- Costa Rica's former Vice Minister of Public Security, Celso Manuel Gamboa Sánchez, three major Costa Rican traffickers, as well as two businesses – one being a football club – involved in narcotics trafficking and the corruption of officials.
- Ryan Wedding (a former Canadian Olympic snowboarder) and nine associates, plus linked businesses, including fuel companies in Mexico, for cocaine trafficking and money laundering using cryptocurrency and high-value, luxury assets.

The Trump administration also used its traditional sanctions toolkit against enablers and facilitators based upstream in the fentanyl and synthetic-opioid supply chain. In September, the US designated a Chinese firm, Guangzhou Tengyue Chemical Company, and two of its staff, Huang Xiaojun and Huang Zhanpeng, for the production and sale of synthetic opioids and for supplying 'cutting agents' used to dilute synthetic drugs (such as nitazenes) to the US market.

The US also targeted those supplying drugs directly online under fronts as 'pseudo-pharmacies;' in September, it designated an Indian business, KS Pharmacy, and its controllers, Sadiq Abbas Habib Sayyed and Khizar Mohammad Iqbal Shaikh, for selling counterfeit prescription fentanyl and methamphetamine to US customers. In addition, the US moved against online market enablers in March, targeting Behrouz Parsarad, an Iran-based administrator of the Nemesis darknet marketplace, which the US Treasury alleged facilitated nearly $30 million in drug sales, including a variety of synthetic opioids, to US buyers between 2021 and 2024.

One further significant area of action for the US in the Americas was against human trafficking and illegal migration networks. In March, it designated Jumilca Sandivel Hernández Pérez, the Mexico-based alleged head of a Guatemalan group, the Lopez Human Smuggling Organization, and in October, the Bhardwaj Human Smuggling Organization based in Cancún, Mexico, along with its senior leadership, and 16 linked businesses. According to the US Treasury, the network, led by dual Indian Mexican national Vikrant Bhardwaj, smuggled illegal migrants from Europe, the Middle East, South America, and Asia into the US using an extensive transport and logistical chain that included the use of yachts and marinas.

This heightened US focus on human trafficking and migrant smuggling is notable when compared to the priorities of other countries. Our survey data shows that 18% of US-based organizations ranked human trafficking and migrant smuggling as one of their top three criminal activities they focused time and resources on in 2025.



This focus is significantly higher than that reported by respondents in other major jurisdictions, including:

- France (15%)
- Canada (13%)
- The UK (13%)
- Singapore (10%)
- Australia (9%)

The elevated priority in the US stems from the Trump administration's policy of framing these networks as a primary national security and immigration challenge. This framing justified the increased use of sanctions and specialized task forces to target the leadership and financial enablers of these organizations in the Americas, forcing US businesses to dedicate greater resources to managing this risk.

> *It is easy to get desensitized in a sea of false positives, but we must remember the goal is to disincentivize traffickers by removing their ability to profit. Financial services firms are uniquely positioned to take on this challenge to follow the money and prevent crimes.*
>
> 
>
> **Taskeen Hamidullah-Bahl**
> STOP THE TRAFFIK

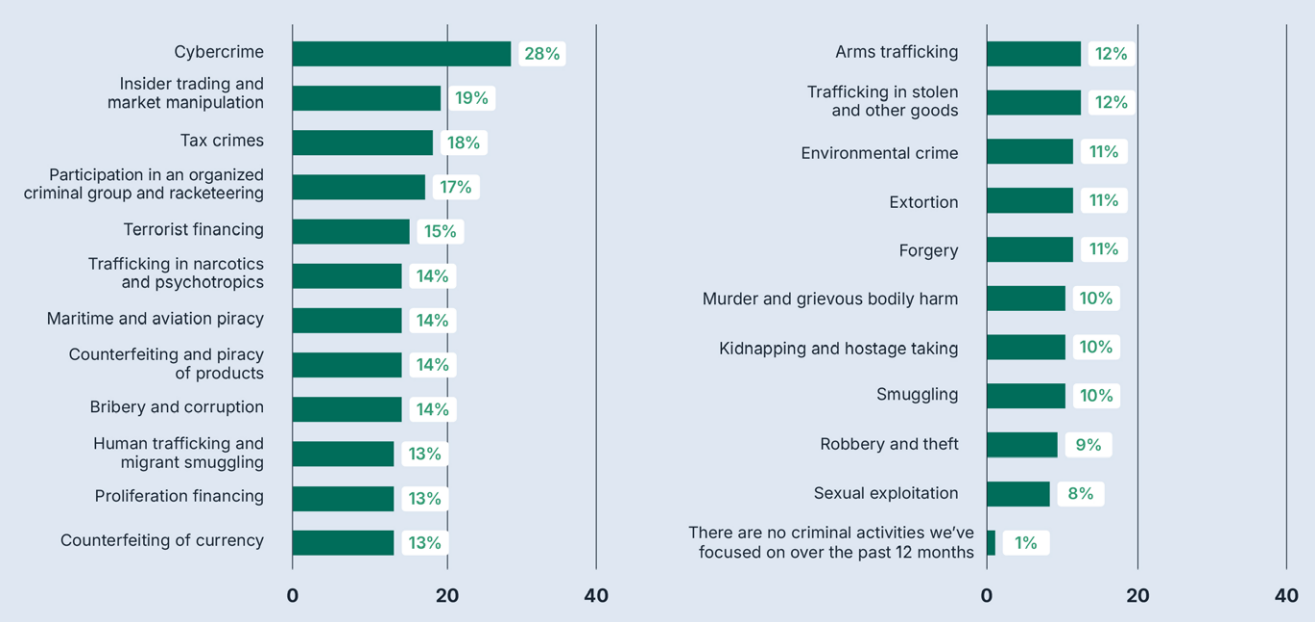
Targeting scam centers

The US looked beyond the Americas as well, with the 'scam centers' of Southeast Asia a significant source of concern. These centers, based around hotel and casino compounds in poorly governed border areas of Cambodia, Laos and Myanmar, used hundreds of thousands of press-ganged and duped workers – often living under the threat of violence – to staff massive phone and online scamming operations targeting victims across the world. These operations typically involved so-called 'pig butchering' schemes, where victims were encouraged to invest increasingly large sums of cryptocurrency – often emboldened by false promises of romance or high returns – in what were actually fraudulent investments (see Chapter 1: Spotlight on financial crime). According to US officials, such scam centers defrauded US citizens of over $10 billion in 2024 alone.

The intense US focus on these networks aligns with the top priorities of organizations globally, as these scam centers are fundamentally cybercrime enterprises. Our survey data shows that cybercrime is the criminal activity that organizations focused the most time and resources on in 2025, ranked highest globally at 28%. The high prioritization is consistent across major jurisdictions, including the US (26%), Canada (22%), the UK (19%), and Australia (31%). The scale of financial loss and the reliance on sophisticated digital fraud techniques explain why US law enforcement and sanctions authorities are treating these geographically distant scam hubs as a tier one financial crime threat.

Many of these centers have been created by international crime groups with their roots in China and Indochina, but they also depended on permissive local elites and insurgent groups in conflict zones for protection and support. The US's first steps came in May, when it designated one such group, the Karen National Army (KNA), a Buddhist militia group in Myanmar, as a transnational criminal organization (TCO); it also designated the group's leader Saw Chit Thu and his sons. In the same month, the US also designated a Philippines-based company, Funnull Technology, and its administrator, Liu Lizhi, for providing online architecture "in bulk" to support the scams, and found Cambodia's Huione Group, a provider of payment services and online marketplaces, to be of "Primary Money Laundering Concern" for its involvement in laundering proceeds both from cyber scams and North Korean cybercrime.

Which of the following criminal activities has your organization focused the most time and resources on over the past 12 months?



Source: ComplyAdvantage, The State of Financial Crime 2026

The US took another substantial set of designatory measures in September, designating nine entities and individuals operating in Shwe Kokko, Myanmar, a leading hub for scam centers protected by the KNA, and ten targets based in Cambodia.

This was followed in October by a joint designation package with the UK targeting 146 individuals and businesses linked to Cambodia's Prince Group, led by Cambodian national Chen Zhi, which the US alleged was one of the major criminal players behind the scam centers.

In parallel, the US also cut off Huione Group from the US financial system. In November, the US took further action, designating another insurgent group – the Democratic Karen Benevolent Army (DKBA), four of its senior leaders, and the Trans Asia International Holding Group Thailand, Troth Star Company, and Thai national Chamu Sawang, alleged to be linked to Chinese organized crime and insurgent groups such as the DKBA. Separate from its application of sanctions, the US also announced an inter-agency 'Scam Center Strike Force,' tasked with dismantling the networks and mitigating risks to US citizens.

Ransomware and bulletproof hosting (BPH)

As noted in previous sections, the proceeds of cybercrime have played a significant role in enabling state actors like North Korea. Cybercrime has overlapped, too, with other domains of serious organized crime, including narcotics trafficking and forced labor. Besides illicit markets like drugs and online scams, another prominent cybercrime wave has persisted in 2025: the deployment of 'ransomware' – a form of malware that encrypts and/or prevents access to a system's data and is used to extort funds from companies (see Chapter 1: Spotlight on financial crime).

This ongoing threat is a major preoccupation for financial crime professionals.

SHARE THIS

Our survey revealed that ransomware is the fourth most concerning financial crime threat for organizations globally over the next 12 months, as cited by 33% of respondents.

This places it just behind long-standing concerns, such as high-end laundering through property and assets (41%) and trade-based money laundering (38%), highlighting the immediate and destructive financial threat posed by these attacks.

The focus on ransomware reflects a broader anxiety over digital financial crime, as 30% of firms also ranked scams as a top concern, while 26% cited the Illicit use of decentralized finance (DeFi). Given that ransom payments are predominantly made using cryptocurrencies and often laundered through DeFi protocols, the great concern across these three typologies underscores a shared risk environment driven by digital rails.

Which of the following financial crime typologies is your organization most concerned about in the next 12 months?

Source: ComplyAdvantage, The State of Financial Crime 2026

In 2025, the US took several actions against ransomware groups and the infrastructure supporting them, in collaboration with international partners. In February, the US, along with the UK and Australia, designated Zservers, a Russia-based bulletproof hosting (BPH) services provider, two of its administrators, and a linked UK front company. BPHs are designed to evade detection and law enforcement interference, and the designating jurisdictions labeled Zservers a leading enabler of ransomware attacks, including those conducted by LockBit, a Russia-based ransomware group, and others using the ransomware variant of the same name. In July, the US designated a further Russia-based BPH, the Aeza Group, which provided cybercrime infrastructure to ransomware groups, illicit marketplaces and data hackers, along with two linked front companies and four group managers; the US and UK took further joint action against Aeza Group's successor, Hypercore Limited, designating the new front company in November. Also in November, and in coordination again with the UK and Australia, the US designated Russian BPH, Media Land, described by the US as a key 'launching pad' for ransomware attacks.

Also of note in 2025 was the targeting of the Russian cryptocurrency exchange Garantex, which US, EU, and UK officials claimed had been responsible for laundering tens of billions of US dollars in illicit funds, including flows linked to Russian sanctions evasion. In August, the US Treasury redesignated Garantex (earlier law enforcement action in March had closed the exchange) and designated its alleged successor company, Grinex, as well as members of its senior management and associated companies in Russia and Kyrgyzstan. The UK joined the US in action against Grinex, while the EU had previously sanctioned Garantex in its 16th Russia package.

Finally, one interesting exception to the growing number of cyber sanctions came in March, when the US delisted the crypto mixer Tornado Cash. Despite insisting that North Korean cyber hackers had used the mixer to launder vast amounts of stolen crypto, the US Treasury decided, in the wake of a court judgment that found it had exceeded its authority in sanctioning software code, to lift the designation.

This unusual case did not affect the overall direction of travel, however, and likely encouraged US officials to be more careful in how they designate CASPs in the future, rather than prohibiting them from doing so altogether.

Organized immigration crime (OIC) and the UK

Migrant smuggling, typically using small boats across the English Channel, has become one of the most controversial political issues in the UK over recent years. In January, then UK Foreign Secretary David Lammy announced that, as part of its response, the UK would create a dedicated sanctions regime to disrupt the criminal networks involved. In July, new measures, the Global Irregular Migration and Trafficking in Persons Sanctions Regulations, were introduced and swiftly put into action. On 23 July, the government designated 25 individuals and entities which it claimed were "at the heart of people-smuggling networks that drive irregular migration to the UK." Those sanctioned included: Iraqi and Kurdish smugglers; Hawala providers accused of enabling illicit payments linked to the smuggling; North African gangs operating in the Balkans and controlling people smuggling routes between North Africa and the EU; several Balkans organized crime bosses; document fraud networks based in Montenegro; and a Chinese inflatable boat manufacturer, alleged to advertise its products "explicitly for people-smuggling." A second round of designations followed in October, scheduled to align with the Western Balkans Summit in London, and designated key enablers of the people smuggling trade, including the Kosovo-linked Krasniqi forgery network, the ALPA illicit finance network, including two of its senior managers, and Nusret Seferović, a Croatian organized criminal whose group supplies other criminals with false Croatian passports. Whether these measures would have their intended effect, of course, remained to be seen. Still, there were few indications of an immediate impact, with the UK Home Office reporting that, at the end of September, small boat arrivals had risen by 53% compared with the previous year ending in September 2024, close to an earlier peak in 2022.

Terrorism

Throughout the year, the UN and national autonomous regimes have continued to maintain their consolidated terrorist lists, adding and removing names regularly. Several significant changes have already been noted above: the rehabilitation of HTS in Syria; further Western designations on Iran and its partner terrorist groups and militias; the targeting of Islamist groups involved in African civil wars; and the US re-badging of several Latin American cartels as terrorist organizations.

Beyond these changes, two additional developments were worth noting. First, in the summer, the US focused its attention on South Asian terrorism. In July, the Department of State designated The Resistance Front (TRF), allegedly a front for the notorious Islamist terrorist group Lashkar-e-Tayyiba (LeT), as an SDGT. The designation followed a terrorist attack in Indian Kashmir in April 2025 for which the TRF claimed responsibility, leading to military exchanges between India and Pakistan. Next, in August, the US designated 'The Majeed Brigade,' an elite wing of the Balochistan Liberation Army (BLA), as an SDGT, after its March hijack of a train travelling between Quetta and Peshawar, in which 31 civilians and security personnel died. This group was not an Islamist organization, however, but an irredentist force seeking to gain Balochi independence from Pakistan, suggesting that the US was seeking to show an even hand between India and Pakistan, by taking measures against two terrorist groups that both sides would separately welcome.

A second area of note was the UK's first application of its Domestic Counter Terrorism (DCT) regime against extreme right-wing groups, with the designation of 'Blood and Honour' in January. In October, this was followed by the designation of alleged neo-Nazi music labels, Embers of an Empire (EoE) and Rampage Productions. Separately, in November, the UK also announced the designation of an Irish Republican splinter group, the 'New IRA,' and one of its alleged financial facilitators.

Human rights and anti-corruption

Since 2012, an increasing number of leading Western jurisdictions – the US, Canada, the UK, Australia, and the EU – have adopted sanctions regimes targeting individuals responsible for human rights abuses and severe corruption. These are commonly described as 'Global Magnitsky' regimes, in honour of Russian lawyer Sergei Magnitsky, who died in pre-trial detention in 2009 after exposing a major tax fraud allegedly involving Russian officials. Throughout 2025, these countries continued to apply their Magnitsky frameworks in a variety of different contexts and for varied purposes already discussed above, for example, targeting:

- Extremist Israeli politicians promoting anti-Palestinian violence.
- Russian officials administering illegally occupied Ukrainian territories.
- Pro-Russian Balkans oligarchs meddling in democratic processes.
- Venezuelan officials and judges suppressing civil liberties and democracy.
- Warring leaders in the Sudanese civil war.
- Scam center bosses and their protectors.

Alongside these examples, Magnitsky-style sanctions were also applied in several other cases. The UK government did so in relatively uncontroversial instances. In March, it designated four former Sri Lankan and ex-Tamil Tiger commanders responsible for serious human rights violations and abuses during the Sri Lankan civil war between 1983 and 2009, while in April, it listed former President of Guatemala Alejandro Giammattei, his associate Miguel Martinez, and the Attorney General Maria Consuelo Porras, members of the so-called 'Pacto de Corruptos' (Pact of the Corrupt). The group was alleged to have profited from significant acts of corruption during Giammattei's term, obstructed attempts to investigate their corruption, and attempted to hinder the 2024 transition of power to President Arévalo. The US, in contrast, made more unexpected use of its Magnitsky regime. Firstly, in January, the outgoing Biden administration sanctioned Antal Rogan, a senior Hungarian government official and ally of Prime Minister Viktor Orbán, for corruption. This caused consternation in Budapest, and the Trump administration, more favorable to Orbán, removed the designation in April. The Trump administration also surprised observers by imposing US Magnitsky sanctions against Brazilian Supreme Federal Court justice Alexandre de Moraes in July. The US stated that this was in response to the judge's unfair treatment of former Brazilian President Jair Bolsonaro during the latter's trial for attempting a coup in 2022. President Trump also imposed import tariffs on some Brazilian goods in July and, in September, designated the Lex Institute, a holding company linked to de Moraes, as well as the judge's wife. In both instances, the use of Magnitsky sanctions has led some observers to ask whether such obviously politicized designations will increasingly become a new tool of US 'lawfare.' In contrast, others wondered whether their use in such circumstances brought the very idea of Magnitsky sanctions into disrepute.

Sanctions evasion structures and trends

The sanctions evasion techniques used by Iran, Russia, North Korea, and other states – including the sale of illicit goods, the purchase of prohibited items, the transportation of those goods and items, and the movement of funds through the financial system in support – have not changed significantly in 2025. Moreover, the methods of the main sanctioned jurisdictions, while not identical, bear striking similarities. This is perhaps not surprising, given the fundamental nature of the globalized economy and international financial system, as well as the increasing political, economic, and security ties between several of these states. Drawing on reports issued in 2025 by law enforcement agencies and regulators, mainstream media, and think tanks, the main elements of sanctions evasion models can be summarized as follows.

Opaque commercial structures

To sell commodities such as oil and purchase prohibited items, including dual-use goods, sanctioned jurisdictions require commercial vehicles that cannot be easily traced back to them. For Iran and Russia, this is usually accomplished through nationals, dual nationals, and trusted third-party nationals setting up 'import-export' or 'general trading' businesses, logistics firms, and consultancies in third-countries or sub-jurisdictions with high levels of trade and numbers of new company registrations, such as the United Arab Emirates (UAE), Hong Kong, and Singapore, to buy and sell goods and commodities. These firms act as intermediaries in the chain of buying or selling sensitive items, keeping producers and consumers at a distance. Interestingly, a July "Red Alert" from the UK's National Crime Agency (NCA) noted that Russian oil sales were managed by two groups of companies with minimal interaction to reduce the risk of discovery: a 'blue' team working with entities in the West, including banks, insurers, and trading platforms and a 'red' team, with obscure ownership structures and disposable front companies which could be dropped if discovered.

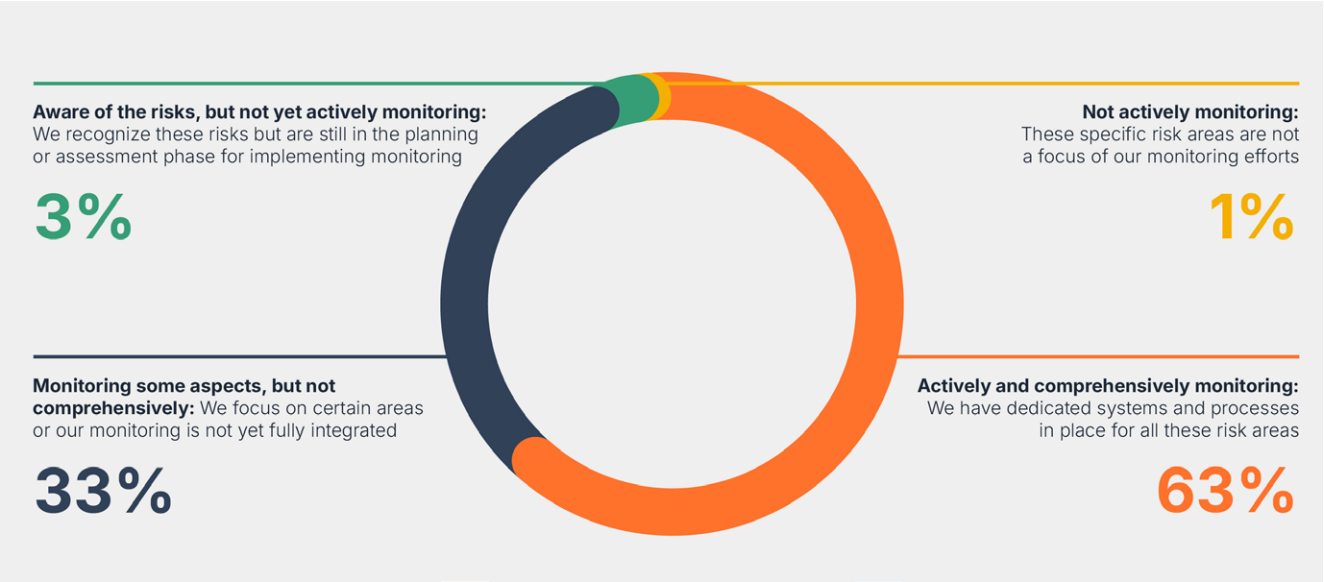
Opaque logistical structures

To deliver their commodities to buyers and receive the restricted goods they have procured, sanctioned states require transport and logistics providers willing to run the risk of detection and interdiction. In contemporary sanctions evasion, the core element is reliance on a shadow fleet of aging tankers. These vessels are usually 'owned' by shell companies in small, poorly regulated third countries and fly flags of convenience. They are also regularly resold, reregistered, and reflagged to obscure their origins. Those managing logistical operations use a range of other measures to obscure their activities, including falsifying trade documentation, misusing HS (Harmonized System) codes to disguise dual-use goods (items with both civilian and military applications), disabling automatic identification systems (AIS) on vessels, and conducting ship-to-ship transfers of sensitive goods in high risk zones such as the Persian Gulf, the South and East China Seas, and the Sea of Japan, to avoid the attention of port authorities.

In light of the increasing complexity of trade-based evasion, the majority of organizations are prioritizing this risk area: our survey data revealed that 63% of firms report having dedicated systems and processes in place for actively and comprehensively monitoring dual-use goods, the misuse of HS/IMO codes, and trade-based money laundering (TBML). However, the remaining 37% of firms either lack full integration, are still in the planning phase, or are not monitoring these specific, high-risk trade evasion vectors at all.

For organizations seeking to enhance trade compliance, the focus should be on integrating and refining data models to address anomalous trade patterns. This requires moving beyond basic transaction screening to implement scenario-based monitoring that effectively links counterparty risk, geographic shipment data, and product classification codes (like HS codes) to build a more robust defense against the evolving logistical structures of sanctions evasion.

To what extent does your organization actively monitor for risks related to dual-use goods, the misuse of HS/ IMO codes for sanctions evasion, and/ or trade-based money laundering (TBML)?



Source: ComplyAdvantage, The State of Financial Crime 2026

Opaque financial structures

To receive funds generated from illicit commodity sales and then to use them for procurement, sanctioned states need to apply financial techniques that do not bring them to the attention of financial institutions, unwitting businesses, law enforcement, or regulators. Increasingly, these financial structures utilize a combination of traditional banking payment rails, informal value transfer systems such as Hawala, which do not involve cross-border fund transfers, and more novel channels like cryptocurrency. Russia still relies heavily on routing funds through multiple correspondent banks to conceal their origin from international financial institutions, but has also developed an informal payments system known as the 'China Track,' where sanctioned Russian banks send and receive payments with Chinese banks via intermediary payment agents in third countries. Iran makes particular use of money exchange houses in the Middle East – businesses that specialize in converting and exchanging currencies – to create complex, layered processes in which illicit funds are routed from exchange houses to regional and national banks, and then through major financial institutions with international correspondent accounts, to get to their intended destination. North Korea, in contrast, maintains a network of foreign-based banking representatives for its sanctioned banks, individuals typically operating under false identities who manage payments through accounts held at Chinese and Russian financial institutions. It should be noted, however, that cryptocurrency is playing an increasingly important role in the financial architecture of sanctions evasion. In its 2025 report, blockchain analytics firm Chainalysis found that in 2024, sanctioned jurisdictions and entities received $15.8 billion in cryptocurrency, accounting for approximately 39% of all illicit crypto transactions. Both Russia and Iran are showing growing signs of adopting crypto to work around the international financial system. Still, at present, the most sophisticated actor remains North Korea, which uses chain-hopping (rapidly moving funds across multiple blockchains) and rapid liquidations of funds via small or lightly regulated exchanges in offshore jurisdictions.

Third-country enablers

A final essential ingredient in contemporary sanctions evasion is the use of third countries – typically non-Western states, but with good relations with Western countries, often in the rapidly emerging markets of the 'Global South' – as locations for buying and selling sanctioned goods. While any such country might be exploited, several regions consistently emerge in publicly available reporting, including those of the Western Balkans (Serbia); the Caucasus (Armenia); the Middle East (Türkiye, the UAE); Central Asia (Kazakhstan, Kyrgyzstan, Uzbekistan); and Southeast and East Asia (Malaysia, Singapore, and China/Hong Kong).

Evasion for sanctioned individuals

Sanctioned individuals have continued to apply well-worn evasion techniques to hide and protect their assets in 2025. The core element remains the re-engineering of beneficial ownership structures, with assets partially or totally transferred to family members, associates and nominees. These changes are typically conducted through trusts, foundations, and other special-purpose vehicles (SPVs) created in offshore financial centers with weaker regulation and managed by intermediary professional enablers in the legal and accountancy professions. Increasingly, these restructuring processes are not 'one-offs' but part of a long-term cycle aimed at staying ahead of sanctioning jurisdictions. Finally, recent law enforcement action has shown **crypto** playing a growing role here too, as a way for designated individuals to move sanctioned funds or launder the proceeds of crime with a lower risk of detection.

Evasion innovation, future trends, and compliance gaps

Sanctions evasion structures largely maintained continuity in 2025, yet new innovations – particularly the use of crypto – are emerging. Three general trends are increasingly evident:

- **Operational integration:** Since the start of the full-scale Russian invasion of Ukraine in 2022, Russia, Iran, and North Korea have all become noticeably closer – politically, economically, and militarily – with China maintaining distance. This closeness is becoming more evident in various ways; the presence of Iranian drones and North Korean troops in Ukraine being the most blatant. However, cooperation and coordination have also manifested in other ways, including in sanctions evasion, where research suggests that, to some extent, these different states have learned from each other's experiences. Moreover, there is an increasing sense that what might be seen as isolated national evasion strategies have begun to evolve into a standard, shared system accessible to or deployable by any state that the West has targeted with economic and financial sanctions.
- **Sanctions evasion-as-a-service (SEaaS):** Allied to this development is what might be seen as the growth of 'sanctions evasion-as-a-service.' This market operates at two levels: the operational and the national. At the operational level, the number of 'service providers' offering corporate, legal, and documentation services, shadow-fleet vessels, and financial facilitation to more than one state has grown. At a national level – and often in tandem – several third countries have, by adopting a relatively lax approach to Western legal and regulatory demands, either knowingly and intentionally or perhaps not, provided relatively safe spaces for evasion. Indeed, some states appear to have become 'one-stop shops' or sanctions evasion 'hubs' for the routing of illicit oil sales and the procurement of dual-use goods.
- **Blending old and new:** While technology is proving increasingly important to all forms of financial crime, what has been notable in the tradecraft of sanctions evasion is how states and criminals have found ways to blend various 'traditional' methods – cash couriering, bank payments, value transfers – with new payment rails and crypto assets (something shown in practice by the Russian money laundering networks disrupted by the NCA's Operation Destabilize). Increasingly, those managing the finances behind sanctions evasion are using hybrid channels, combining them into extensive, convoluted chains of transactions and shifting funds between them at high speed.

These trends are expected to continue in 2026 and beyond, with the integration among Russia, China, and Iran expanding across various domains. The chances are, moreover, that a broader range of states – Middle Powers such as Brazil, India, South Africa, which already have close economic relationships with Russia and China through economic groups such as BRICS – will look to ensure they have access to any developing alternative financial systems that sit alongside the US dollar-backed traditional banking network. This might include a broader shared use of crypto assets such as stablecoins, emerging central bank digital currencies (CBDCs), or even a common digital currency.

The continuation of several extensive Western sanctions regimes is also likely to further fuel the 'sanctions evasion-as-a-service' market, as integration among commercial, legal, and logistical enablers deepens. Indeed, intermediaries sitting in 'one-stop shop' evasion hubs will likely become more central to the overall evasion ecosystem, with the best becoming 'go-to' providers that command high fees. It is also likely that, as with any developing market, there will be both consolidation and ongoing innovation; one probable development will be the growing 'bundling' of several evasion services by providers. As long as the world remains geopolitically divided, many neutral governments are unlikely to take substantial action, especially if their countries' economies can benefit. Indeed, several are likely to position themselves intentionally as hubs for fast incorporation and financial innovation. While this trend will continue in familiar regions such as Central Asia and the Middle East, it is also likely to diffuse to more 'cut-out' zones in West Africa, the Caucasus, or Southeast Asia.

The potential future impact of technology on evasion also needs to be acknowledged. While the blending of old and new will continue, the advances of technology and human ingenuity in its application will almost certainly open wider opportunities for sanctions evaders. Crypto will become more critical as its adoption expands, as will offshore exchanges and over-the-counter (OTC) brokers in lightly regulated third countries. The mixed use of crypto, stable coins, and privacy coins, decentralized peer-to-peer transactions, and transactions between different blockchain infrastructures, though difficult, will become more common, making it more difficult for conventional blockchain analytics methods to work effectively.

Generative AI will also continue its current trajectory and potentially become a force multiplier for sanctions evaders. The potential number of options it can add to the evaders' repertoire is concerning, including but not limited to:

- Creating synthetic identities and commercial documentation to work around individual and business customer due diligence (CDD) requirements or construct plausible beneficial-ownership chains (as noted in Chapter 1: Spotlight on financial crime).
- Developing sanction-resistant pathways and transaction-layering patterns designed to mimic legitimate trade and financial flows and thus skirt automated transaction monitoring and sanctions screening filters
- Identifying vulnerabilities in Western regulations, controls, and enforcement, and road-testing hypothetical sanctions evasion scenarios to assess their potential effectiveness.

3D printing technology and the growth of distributed manufacturing will also help evaders. For example, local production of dual-use components based on shared blueprints and designs in evasion hubs will enable evaders to quickly supply 'in-demand' items or avoid using supply routes for certain items where there is a high risk of interdiction. In combination, therefore, the ongoing fragmentation of the geopolitical landscape, the development of sanctions evasion providers as businesses, and the advance of new technology will pose new challenges to Western regulators, law enforcement agencies, and businesses that will be difficult to address without radical thinking.

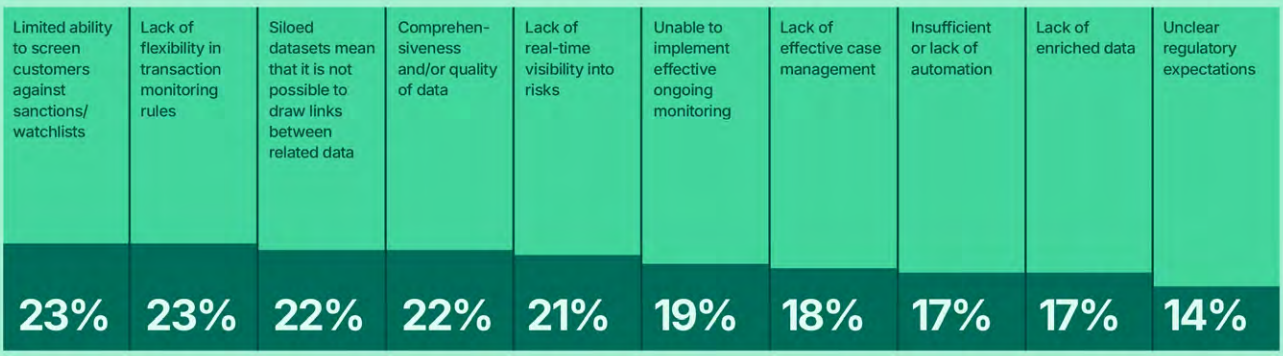
Compliance gaps: Technological and data limitations

The capacity to detect these threats is compromised by persistent technological and data limitations. Our survey of compliance professionals in 2025 highlights these structural issues: the two most cited limitations were:

1. Limited ability to screen customers against sanctions/ watchlists (23%).
2. Lack of flexibility in transaction monitoring rules (23%).

This difficulty in core customer screening is often a symptom of underlying data hygiene and systemic fragmentation – with 22% also citing "siloed datasets" and "comprehensiveness and/or quality of data" as major hurdles. Poor data quality and fragmented ownership structures hinder accurate sanctions list matching, resulting in high rates of false positives and the potential for genuine matches to be overlooked.

What are the main limitations to your organization's current approach to financial crime detection?



1% | There are no limitations to my organization's current approach to financial crime detection

Source: ComplyAdvantage, The State of Financial Crime 2026

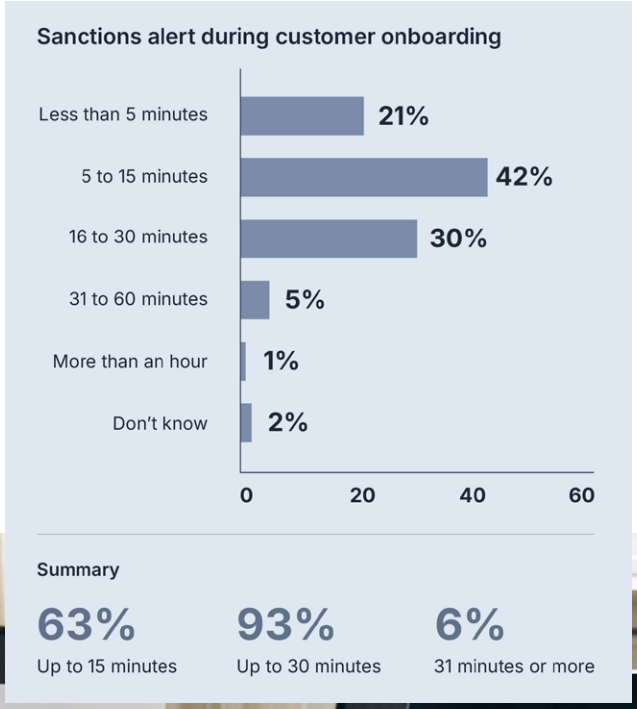
SHARE THIS

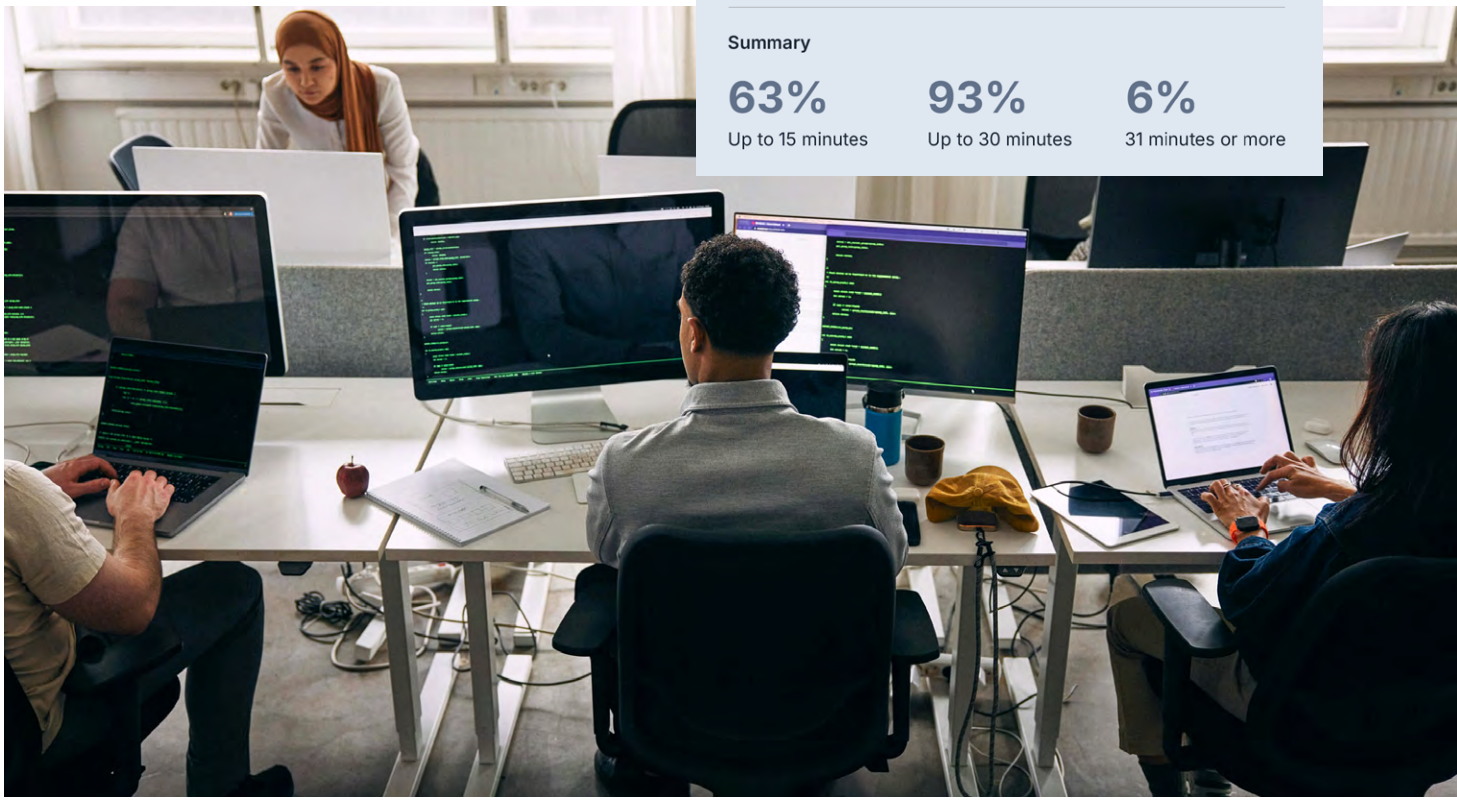
Similarly, the cited “lack of flexibility in transaction monitoring rules” is a technical bottleneck.

Reliance on static, rules-based scenarios is quickly compromised by sophisticated actors, necessitating a shift toward behavioral analytics and predictive modeling to detect novel evasion typologies.

The operational cost of these limitations is starkly evident in remediation times: 79% of respondents reported that remediating a sanctions alert during customer onboarding takes more than 5 minutes (with 36% taking 16 minutes or more). This inefficiency signals a strong reliance on manual review and a failure of current matching algorithms to effectively handle transliteration, aliases, and false positives at speed.

Approximately, how long on average does it take your organization’s compliance team to remediate the following alerts?





Source: ComplyAdvantage, The State of Financial Crime 2026

What does this mean for my firm?

As the last five years have shown, making geopolitical predictions can feel like an exercise in futility. The course of history continues to surprise us, and 2026 is as likely to do so as 2025. Based on current trends, even if some wars are partially resolved through the peace initiatives of President Trump and others, tensions in Europe, the Middle East, Latin America, sub-Saharan Africa, and East Asia will persist. Indeed, it is highly plausible that some of them will erupt into conflict. Which, however, is impossible to say; in the world as it now is, the unexpected can arrive quickly. President Trump made various comments throughout 2025 about the US's need to buy (or even annex) **Greenland** from Denmark, and suggesting that **Canada** should join the US for its own security. While some have seen these statements as little more than idle musings from President Trump, there is every chance he might seek to act upon them in 2026 (indeed, in the case of **Greenland** that increasingly seemed the case in early January). Businesses must therefore remain vigilant about developments in high-risk regions, particularly those to which they are exposed.

Businesses will thus need to stay informed about the trajectories of sanctioning jurisdictions. In the current climate, the UNSC is near certain to remain gridlocked, with no new action emerging on either North Korea or Iran. At the level of autonomous national and multilateral sanctions regimes, the US seems likely to make ever-greater use of tariffs as an all-purpose means of coercion; President Trump will use sanctions selectively to put pressure on third parties and third countries evading existing regimes, and to target those who challenge his policy priorities – particularly the organized crime groups behind various streams of illicit trafficking into the US. In contrast, the EU, UK, Canada, and Australia are likely to remain broadly aligned, renewing and expanding existing regimes on Russia and Iran, while also using additional secondary measures to counter sanctions evasion through third countries. Although the US and 'the rest of the West' are unlikely to diverge radically on sanctions in 2026, differences of style and emphasis will become more obvious.

As noted above, businesses will also need to be watchful for changes in the methods and typologies of sanctions evaders. Thought will be needed about how to mitigate risks from emerging non-traditional sanctions evasion vectors and techniques, such as the emergence of third country evasion 'hubs' and sanctions evasion service providers, the abuse of new payment rails and crypto assets, and the exploitation of generative AI to help 'professionalize' many aspects of sanctions evasion. Although watching for classic red flags of sanctions will remain crucial, businesses cannot rely on them alone.

Iain Armstrong
Executive Director, FCC Strategy, ComplyAdvantage

What does this mean for my firm?

Businesses will also need to consider how well-equipped they are to detect such developments with their existing technology stack. CDD needs to adapt to fluid corporate structures and identity abuse, moving beyond static onboarding to integrated KYC systems. To improve efficiency and detection, firms should focus on strategic technology upgrades:

- Revisit rules-based transaction monitoring and static name-matching sanctions screening platforms. In the first case, they should consider turning to systems that can dynamically identify abrupt changes in customer behaviour.
- Examine deploying systems that provide automated near real-time ingestion of sanctions list updates, advanced fuzzy matching, and an ability to discern the kind of transliteration manipulation often seen in Russian, Persian, and Korean naming conventions.
- Complement obligatory monitoring with adverse media screening to proactively identify high-risk individuals and entities before they are officially designated, thereby moving the firm from a purely reactive stance to a preventative one.

In today's uncertain world, firms should aim to prevent financial crime risk rather than only mitigate it.

Andrew Davies
Head of Global FCC Strategy, ComplyAdvantage

Back to beginning
Previous section
Next section

Regional regulatory trends

Global

The Financial Action Task Force (FATF)

Firms should closely follow the work of the Financial Action Task Force (FATF), an intergovernmental body that sets global standards for AML/CFT, which will continue to issue guidance and reports at a rapid pace. These publications include case studies, threat indicators, red flags, and typologies in areas identified as threats to the global financial system and align with the priorities set under the Mexican Presidency for 2024-2026:

- Financial inclusion.
- Strengthening the Global Network.
- The effective implementation of the FATF Standards.

Specific areas of focus include:

Technical standards

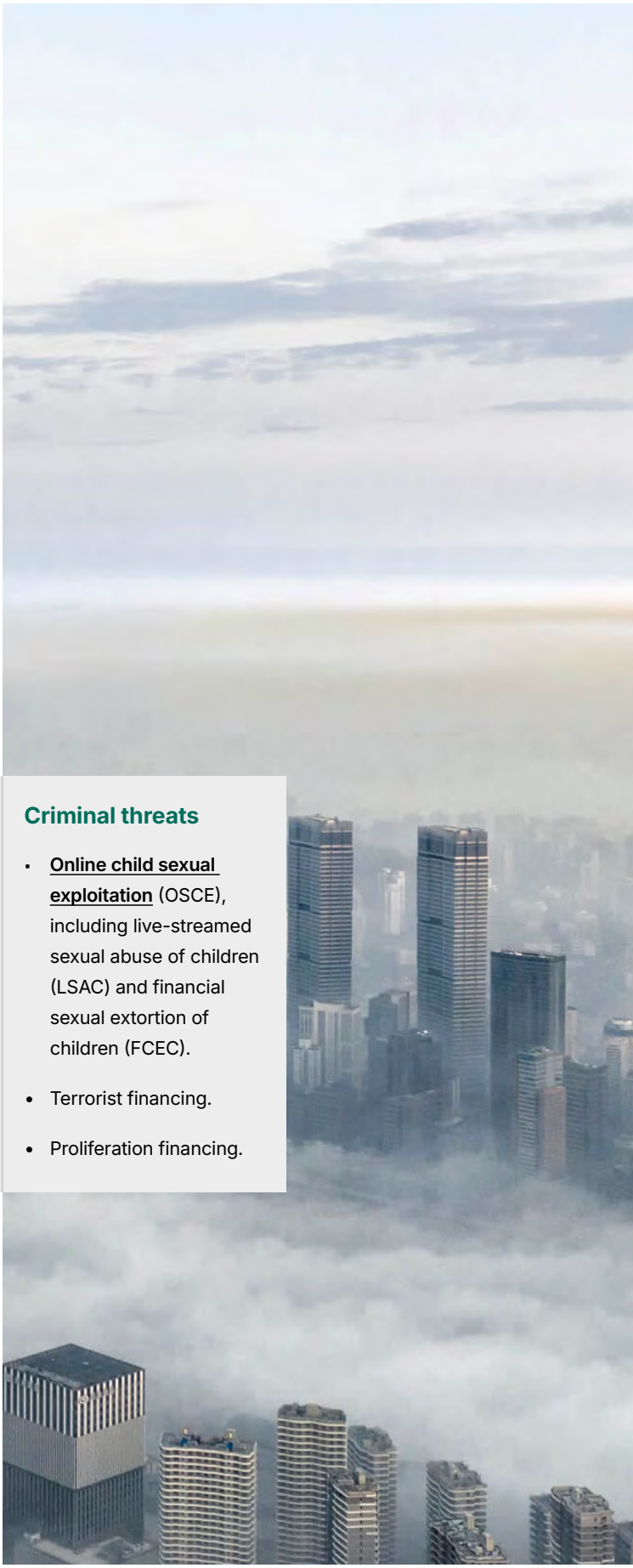
- Risk-based approach (RBA) to address de-risking.
- Asset recovery.
- Beneficial ownership.

Financial systems

- Virtual asset service providers (VASPs)/crypto.
- Cross-border payments.

Criminal threats

- **Online child sexual exploitation** (OSCE), including live-streamed sexual abuse of children (LSAC) and financial sexual extortion of children (FCEC).
- Terrorist financing.
- Proliferation financing.



The FATF has also cited fraud as "one of the fastest growing threats on a global scale" and recommends that firms treat it as an emerging threat.

Firms should review the new FATF reports published to respond to illicit finance risks. This includes reports on proliferation financing and sanctions evasion, as well as its global assessment of terrorist financing risks and implementation of FATF standards related to virtual assets and virtual asset service providers (VASPs).

To facilitate access to financial services by the 1.4 billion unbanked, the FATF recently updated Recommendation 1 on the RBA. It has issued updated guidance for firms to "boost financial inclusion," including measures to apply simplified due diligence (SDD) in low-risk situations and simplify identification sources, documents, and other information requirements. The FATF also published a national risk assessment toolkit to guide countries, including those with low capacity, on how to apply the RBA. The findings of these national assessments are a critical resource for firms to consider when updating their own enterprise-wide risk assessments. The FATF also revised its procedures for carrying out mutual evaluations to address the unintended consequences of the misapplication of the FATF Standards on non-profit organizations (NPOs), such as illegitimate targeting and suppression, while also protecting NPOs from terrorist financing.

Regarding financial transparency, the FATF expanded the scope of Recommendation 16 (R16) from wire transfers (typically associated with traditional cross-border payments) to promote payment transparency more broadly. R16, also known as the 'Travel Rule' in the crypto space, includes standards around originator and beneficiary information that must accompany payments or value transfers. Key changes include:

- Clarification on who is responsible for including certain information along the payment chain.
- Introducing standardized requirements on the information (name, address, and date of birth) that should be included in cross-border, peer-to-peer payments above USD/EUR 1,000.
- Carving out credit, debit, and prepaid card transactions used to buy goods and services from R16 requirements.
- Expanding the requirement to freeze prohibited transactions related to payments to "the prevention, suppression and disruption of proliferation of weapons of mass destruction."
- Introducing requirements in the Interpretative Note to R16 for financial institutions to "introduce tools that protect against fraud and error."

Countries are expected to implement changes by the end of 2030, and the FATF is expected to issue updated guidance.

The FATF also regularly updates its list of high-risk jurisdictions subject to a call for action (the 'black list') and jurisdictions under increased monitoring (the 'grey list'). In October 2025, the watchdog removed Burkina Faso, Mozambique, Nigeria, and South Africa from the list of jurisdictions under increased monitoring after they had completed their Action Plans. Russia's membership of the FATF remains suspended.

In our survey, when senior compliance professionals were asked, "Which of the following FATF grey list countries is your organization most concerned about?", the top three responses, collected prior to South Africa's removal in October 2025, emphasized a concern rooted in political and governance instability.

- Syria (23%)
- South Africa (22%)
- Democratic Republic of Congo (22%)

Which of the following FATF grey list countries is your organization most concerned about?

Source: ComplyAdvantage, The State of Financial Crime 2026

SHARE THIS

The timing of this data offers an interesting gauge of the grey list's actual operational impact.

The fact that South Africa was the second-highest concern (22%) right up until its de-listing confirms the sustained compliance burden and management anxiety that persists even as a country nears the threshold for official compliance.

The top concern regarding Syria (23%) is likely rooted in the material regulatory risk created by the country's recent geopolitical transformation. Syria remains on the FATF grey list, a status that has been significantly complicated by the December 2024 collapse of the Assad regime and the establishment of a new transitional government. This concern is driven by the country straddling two distinct statuses for financial institutions:

- **The economic opportunity:** Regime change is widely expected to lead to the opening-up of the economy and attract reconstruction capital. The US has significantly reduced economic pressure – notably by revoking six prior Executive Orders and suspending secondary sanctions under the Caesar Act – signaling clear intent for renewed regional engagement.
- **Persistent risk:** The core exposure remains significant. While its implementation is suspended, the Caesar Act's full repeal is still pending in the US House of Representatives (as of late 2025), leaving the door open for sanctions reintroduction. Compounding this is the profound governance deficit: the new transitional government faces a mountain to climb in establishing robust regulations aimed at corruption and money laundering, and scaling up corporate governance generally.

Wolfsberg Group

The Wolfsberg Group, comprising twelve of the world's systemically important banks, will continue to issue updated guidance and resources for banks to follow. It is strongly recommended that financial institutions review developments and that firms operating in other sectors also review Wolfberg Group updates to inform the development of their own internal AML/CFT systems and controls.

In 2025, the Wolfsberg Group issued the following guidance and statements:

- Statement on the RBA, calling for proportionality, prioritization, and effectiveness
- Statement on Effective Monitoring for Suspicious Activity, issuing a responsible framework for innovation, which included the following three core pillars: (1) transition and validation; (2) balancing model risk with financial crime risk; and (3) explainability to demonstrate transparency in coverage and effectiveness.
- Guidance on the Provision of Banking Services to Fiat-backed Stablecoin Issuers, which sets out a financial crime risk framework for banks offering services such as operating accounts, reserve management, and client settlement to fiat-backed stablecoin issuers. The guidance highlights that "most of the same financial crime risk management principles apply". Still, it establishes a framework for financial institutions to manage financial crime risks that are unique to having a stablecoins issuer as a client. This includes understanding: the minting/burning approach for client settlements; how the issuer applies the Travel Rule to digital asset service providers (DASPs); the extent of on-chain monitoring carried out; controls around unhosted wallets; the use of smart contracts to verify wallet addresses and block transactions; and the use of privacy-enhancing technologies.

What does this mean for my firm?

Firms should review key documents issued by the FATF to help identify key risk indicators and support the update and/or development of their enterprise-wide risk assessments. Firms should also refer to the FATF risk-based guidance to identify instances where SDD can be applied and to recognize examples of overcompliance. Firms should also review their internal policies and procedures to incorporate updates to FATF standards into their internal systems and processes as they become legal or regulatory requirements in their countries of operation.
This should entail carrying out a gap analysis, impact assessment, and developing an implementation roadmap, especially when changes involve technology solutions. Firms should ensure relevant staff are trained on key changes.

Regarding the Wolfsberg Group statements and guidance, firms may find it helpful to review the statements and determine if any calibrations can be made to their AML/CFT programs, particularly to their risk-based models and suspicious activity monitoring systems, and controls. Any firm (including crypto-asset service providers) offering services to stablecoin issuers should review the guidance on stablecoins to identify the steps the banking industry has agreed should be taken to manage risks effectively, as well as to understand what evidence firms will need to provide to their banking partners.

Andrew Davies
Head of Global FCC Strategy, ComplyAdvantage

Technology is evolving so rapidly, but so are the fraudsters, and they don't care. It's really important as a business that we do care, and we take the necessary steps that we need to. Yes, it's going to cost more in the short term, but in the long term, if you're improving customer experiences, building customer trust, building the reputation of your brand, these are all great things.

Dane Pedro
Head of UK Compliance & MLRO, Mollie

Hear more from Dane in our on-demand virtual conference series: *The Future of Payments Summit*

North America

North America will continue to see changes to laws and regulations as the FATF carries out its mutual evaluation reviews (MER) to assess the effectiveness of national AML/CFT/CPF frameworks in 2025/2026. Canada's MER was launched in November 2025 and will continue into 2026. The United States' and Mexico's mutual evaluations are both scheduled to begin in February 2026.

United States

In the United States, firms can expect to see both a drive towards deregulation as President Trump's policies take hold and more clarity around regulation in the crypto space. On January 31, 2025, the White House issued an Executive Order on "unleashing prosperity through deregulation," to address increasing compliance costs and the risk of non-compliance costs. This announced a key policy of the Trump administration to lower costs for parts of the private sector required to comply with federal regulations, aiming to "secure America's economic prosperity and national security." For every new regulation issued, the government is mandated to identify at least ten prior regulations for elimination to offset the costs. This is likely to yield a flurry of activity in the regulatory space to "alleviate unnecessary regulatory burdens."

Key regulatory developments from the US to be aware of are set out below.

Beneficial ownership

On March 2, 2025, the US Treasury announced that it would narrow the scope of the Corporate Transparency Act (CTA) to foreign reporting companies only and would not enforce any previous penalties or fines for failing to comply with the beneficial ownership reporting rule.

Banks

On June 27, 2025, the US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued an Exemption Order containing a change that may affect the customer due diligence (CDD)/know your customer (KYC) policies and procedures for banks. The order allows banks to collect taxpayer identification number (TIN) information from a third party instead of only the customer.

Digital assets & crypto

The US government enacted the Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act on July 18, 2025, setting out a framework for regulating payment stablecoins. The GENIUS Act is set to support "responsible growth" and the use of digital assets by encouraging innovation in payment stablecoins while protecting consumers and managing illicit finance and financial stability risks. This is a key initiative to support Executive Order (EO)14178 on "strengthening American leadership in digital financial technology."

Effective July 18, 2028, crypto exchanges and firms may only offer a payment stablecoin in the US that is issued by a permitted payment stablecoin issuer (PPSI) or a foreign payment stablecoin issuer (FPSI) that meets specific criteria.

The GENIUS Act established three categories of PPSIs, including: (1) subsidiary of an insured depository institution; (2) a federal qualified payment stablecoin issuer; or (3) a state qualified stablecoin issuer. Under the GENIUS Act, the US Treasury has been tasked with introducing limits on the issuance of payment stablecoins, creating rules to determine whether state-level regulation is similar to federal regulation, and assessing whether a foreign country's stablecoins regime is comparable to the US regime. States will only be able to regulate PPSIs with stablecoin issuance of less than $10 billion. Other federal authorities have been tasked with implementing capital and liquidity requirements (currently set at a one-to-one basis using US dollars or similarly liquid assets), creating a licensing and supervisory framework for PPSIs, and drafting regulations for depository institutions that hold stablecoin reserves or that participate in stablecoin activities. PPSIs and FPSIs will need to publish their redemption policies and information about their reserves each month. The bill also includes requirements around reusing reserves and providing safekeeping services for stablecoins.

A consultation on detecting illicit activity involving digital assets was launched in late 2025. It specifically asked for input on innovations, techniques, or strategies that regulated financial institutions use, or could potentially use, to detect illicit activity involving digital assets, as well as information on application programming interfaces, artificial intelligence, digital identity verification, and blockchain technology and monitoring.

The US also indicated that it would establish a Strategic Bitcoin Reserve and the United States Digital Asset Stockpile on March 6, 2025. The Strategic Bitcoin Reserve consists of BTC obtained through criminal or civil asset forfeiture and other civil money penalties not subject to any other executive or legal action. At the end of October 2025, it was reported that the Strategic Bitcoin Reserve held over 327,000 Bitcoin following the seizure of BTC valued at over $15 billion linked to the forced labour cryptocurrency scams compound owned by the Prince Group in Cambodia. The Digital Asset Stockpile, which now has its own administrative office to manage its custodial accounts, was set up to support the management of digital asset holdings of the US.

Investment advisers

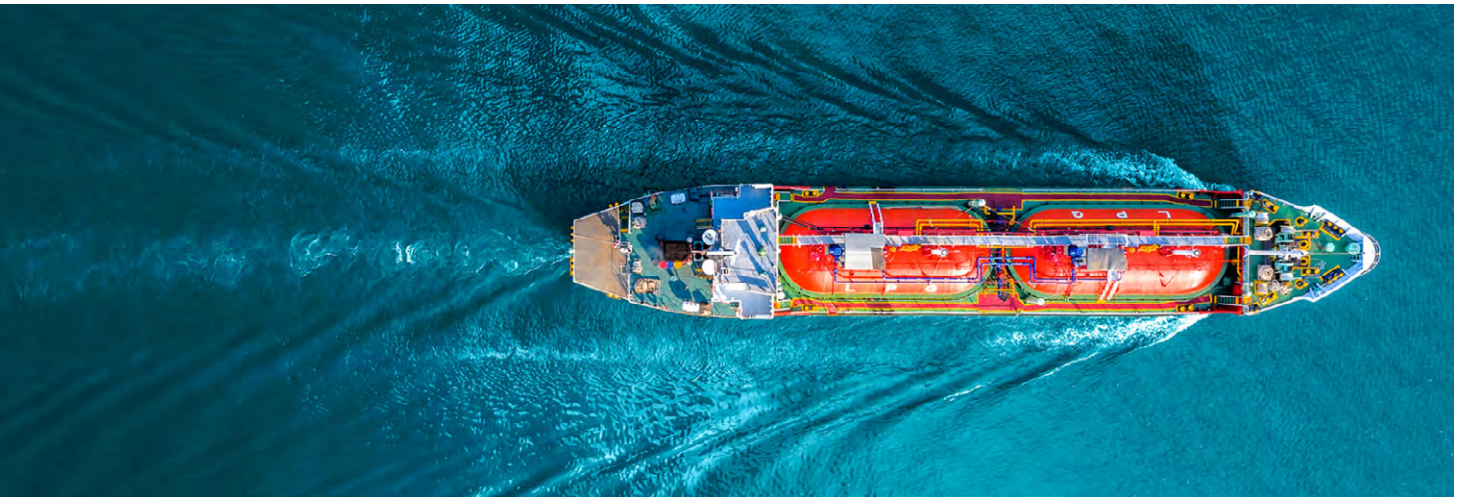
In the investment adviser space, FinCEN announced that it would postpone the implementation date of the final rule, the Anti-Money Laundering/Countering the Financing of Terrorism Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers and Exempt Reporting Advisers (IA AML Rule), from January 1, 2026, to January 1, 2028. The rule was drafted to address illicit finance risks in the investment advisers space. During this time, the scope of the rule will be subject to review, including the substance of the IA AML rule and the requirements surrounding the creation of a customer identification program. It is anticipated that direct costs as a percentage of total operating expenses to comply with the Bank Secrecy Act (BSA) and Office of Foreign Assets Control (OFAC) sanctions regulations will also be assessed as part of the review.

Non-bank financial institutions (NBFIs)

FinCEN is expected to publish results from its Survey of the Costs of AML/CFT Compliance, which closed in December 2025. The survey was developed to gather information on the direct costs faced by non-bank financial institutions (NBFIs) to advance deregulatory proposals "to reduce compliance burden without compromising the effectiveness of current AML/CFT frameworks." NBFIs covered include: casinos and card clubs (casinos); money services businesses (MSBs); insurance companies; dealers in precious metals, precious stones, or jewels (PMSJs); operators of credit card systems; and loan or finance companies.

Real estate

FinCEN recently announced that it would postpone the reporting requirements under the Anti-Money Laundering Regulations for Residential Real Estate Transfers Rule (RRE Rule) to March 1, 2026. The rule requires "persons involved in real estate closings and settlements" to file reports that "are highly useful in criminal, tax, or regulatory investigations or proceedings" or in the conduct of "intelligence or counterintelligence activities, including analysis, to protect against international terrorism." This postponement has been announced to give the industry more time to comply, reduce costs, and protect against money laundering, terrorist financing, and other serious illicit finance threats.



Alerts & enforcement

FinCEN will continue to issue alerts, advisories, analyses, and orders to put regulated firms on alert to identify and report suspicious activity and transactions, thereby mitigating money laundering and terrorist financing risks. In 2025, FinCEN issued the following:

- March 11, 2025: Southwest border geographic targeting order (GTO) to combat illicit activities and money laundering carried out by Mexican cartels and criminal actors.
- March 31, 2025: Alert on bulk cash smuggling (BCS) and repatriation by Mexico-based transnational criminal organizations (TCOs).
- April 1, 2025: Advisory on the financing of the Islamic State of Iraq and Syria (ISIS) and its global affiliates.
- April 9, 2025: Financial trend analysis on fentanyl-related illicit finance.
- April 14, 2025: Numerous residential real estate geographic targeting orders were renewed, which mandate a US title insurance company to identify the beneficial owners behind shell companies used to purchase real estate in certain counties and metropolitan areas.
- May 1, 2025: Alert on oil smuggling schemes on the US southwest border associated with Mexico-based cartels.
- May 1, 2025: Designation of primary money laundering concern for Cambodian-based Huione Group to combat cyber and crypto scams and heists.
- May 6, 2025: Advisory on the Iranian regime's illicit oil smuggling activities, shadow banking networks, and weapons procurement efforts.
- June 25, 2025: Designated CIBanco S.A., Institution de Banca Multiple (CIBanco), Intercam Banco S.A., Institución de Banca Multiple (Intercam), and Vector Casa de Bolsa, S.A. de CV (Vector) as being of primary money laundering concern due to links with illicit opioid trafficking.
- August 4, 2025: Notice on the use of convertible virtual currency kiosks for scam payments and other illicit activity, which also refers to the use of crypto ATMs.
- August 28, 2025: Advisory on the use of Chinese money laundering networks by Mexico-based transnational criminal organizations to launder illicit proceeds.
- August 28, 2025: Financial trend analysis on Chinese money laundering networks.
- September 5, 2025: Guidance on cross-border information sharing to promote cross-border information sharing between financial institutions.
- September 8, 2025: Notice on financially motivated sextortion.
- November 28, 2025: Alert on cross-border funds transfers involving illegal aliens.

FinCEN is also likely to issue a limited number of fines for violations of the BSA in 2026. In 2025, it issued a civil penalty against a firm for failing to register as an MSB and for not developing, implementing, and maintaining an effective AML program.

Canada

As Canada continues to implement its 2023–2026 strategy and the Financial Action Task Force (FATF) mutual evaluation review (MER) process takes hold, new changes will be rolled out to strengthen Canada's AML and anti-terrorist financing (ATF) framework throughout 2026. This follows an investment of more than $379 million over five years into enhancing Canada's AML/ATF regime.

In 2025, Canada announced regulatory amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations and the Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations. The amendments are aimed at enhancing the effectiveness of its national framework to improve efforts in combating money laundering linked to transnational crime and the trafficking of drugs. Changes include:

- Increasing the authorities of the Canada Border Services Agency to "reinforce its ability to detect, deter, and disrupt trade-based financial crime."
- A new framework to facilitate private-to-private information sharing of suspected money laundering, sanctions evasion, and terrorist financing, and public-private information sharing with the new Integrated Money Laundering Intelligence Partnership (IMLIP).
- A new discrepancy reporting requirement to flag anomalies between the beneficial ownership registry maintained by Corporations Canada and private firms.
- Extension of AML/ATF obligations to factoring companies, cheque cashing businesses, and finance and leasing companies.

Tackling the international and domestic illegal drug trade and drug trafficking, including fentanyl, will remain a priority. The government of Canada also released its national risk assessment (NRA), the 2025 Assessment of Money Laundering and Terrorist Financing Risks in Canada. The NRA draws attention to organized crime groups and third-party enablers as key money laundering threat actors driving illegal drug trafficking and fraud. Higher ML threats in Canada include commercial trade fraud, trade-based ML, and tax crimes.

On July 28, 2025, FINTRAC issued a fine of CAD $19,552,000 against a cryptocurrency exchange for failing to register as a foreign MSB, to report virtual currency transactions exceeding $10,000, and to submit suspicious financial transactions.

Mexico

As Mexico ramps up activity before its FATF mutual evaluation, it will continue to implement reforms enacted in 2025. Mexico recently amended the Federal Law for the Prevention and Identification of Transactions Involving Illicit Funds (LFPIORPI). The new law contains the following updates:

- It expands the scope of AML/CFT requirements to Trusts, requiring trustees and fiduciaries to have in place CDD/KYC, transaction monitoring, and record-keeping policies and procedures.
- Real estate developers, agents, and intermediaries have been identified as carrying out "vulnerable activities" requiring them to have AML/CFT programs in line with detailed requirements.
- Crypto exchanges and VASPs now also fall within the scope of AML/CFT rules.
- The beneficial ownership threshold has been lowered from 50% to 25% and there is now a requirement for controlling beneficiaries to register with the national corporate registry.
- Record-keeping requirements have been set for 10 years.
- Firms must carry out an annual review or audit to assess compliance with legal obligations.
- AML/CFT responsible compliance officers are required to receive AML/CFT training on an annual basis.

National authorities have 12 months to develop additional guidance on these changes.

Europe

European Union

AML Package

The EU continues to roll out the AML Package, developed to harmonize rules across member states and strengthen the EU's ability to tackle money laundering and terrorist financing. The AML Package consists of four separate legal instruments:

1. The Anti-Money Laundering Authority Regulation (AMLAR), creating the Authority for Anti-Money Laundering and Countering the Financing of Terrorism;
2. The AML Regulation (AMLR), setting out AML/CFT requirements for the private sector;
3. The 'new' 6th AML Directive (6AMLD), which sets national requirements to harmonize legal AML/CFT frameworks; and
4. The Transfer of Funds Regulation (ToFR), which extends the Travel Rule to crypto and payment transparency requirements.

Both countries and firms will need to ensure that they are aware of implementation dates and of the various supporting documentation as it is released across the region.

The below provides a timeline for key dates for implementation of the AML Package:

Source: Baker Mackenzie

Specific updates include:

1. AMLA

The AMLA has been established as a supra-regional authority to lead the harmonization of the EU's efforts to combat money laundering. AMLA recently published a paper setting out its vision and work program. In addition to setting up its headquarters in Frankfurt, it will lay the foundation for AML/CFT supervision and policy work on risk and measures and build "a strong, connected, and future-proof EU framework for financial intelligence."

Starting January 1, 2028, it will directly supervise 40 systemically important financial institutions deemed to be high-risk and serve as a central coordinator for cross-border cases.

AMLA will issue risk-based supervisory guidelines by July 10, 2028. AMLA will also issue guidelines by July 10, 2029, detailing criteria for and how to assess knowledge and expertise, as well as how to determine that senior managers and beneficial owners of certain entities act with honesty and integrity. Starting on July 10, 2028, AMLA will issue an opinion on ML/TF risks affecting the EU, which will be reviewed every two years.

2. AML regulation

Obliged entities will need to ensure that they are compliant with the AMLR by July 1, 2027. Sectors that will be covered by AML/CFT regulations now include: crypto-asset service providers, crowdfunding platforms, certain types of intermediaries, professional football clubs and agents, dealers in precious stones and metals, dealers in high value goods, and legal professionals facilitating certain higher risk transactions, non-financial mixed activity holding companies, trust and company service providers, and investment migration operators. Traders in ordinary goods will no longer be included. Additional changes include: the need to appoint a board-level AML compliance manager, separate to an AML compliance manager, to promote senior management responsibility and the need to have group-wide policies and procedures; clarification of outsourcing arrangements; application of limits of cash payments to €10,000; the requirement to have in place sanctions compliance programmes; harmonized identification and verification requirements; expanded simplified due diligence and enhanced due diligence (EDD) measures; application of customer due diligence (CDD) requirements for transactions over €10,000; and a requirement for CDD refresh for customers at least every 5 years.

3. 6th AML Directive

Member states must implement the new 6AMLD by July 10, 2027. Access to beneficial ownership registers applying the principle of legitimate interest needs to become available by 10 July 2026. By July 10, 2028, countries will also need to start publishing an annual list of sectors to which the AML regulations apply and adopt risk-based AML/CFT measures to grant residency for investment programs. By July 10, 2029, countries will also need to: (1) establish single access points for information on real estate registers; and (2) ensure that centralized automated mechanisms which support the identification of holders of payment, securities, crypto and other types of accounts and safe deposit boxes are interconnected via the bank account registers interconnection system (BARIS) which the European Commission will develop. The new 6AMLD also increases penalties for non-compliance to €10 million or 10% of annual turnover (whichever is higher).

4. ToFR

Under the ToFR, the European Commission will issue a report assessing the risks associated with transfers involving self-hosted wallets and options for mitigating those risks by July 1, 2026. This may lead to the ToFR being amended.

EU payments landscape

On the payments front, the European Council has prioritized creating a fully integrated instant payments (IPs) market. Updated Regulation (EU) 2024/886 as regards instant credit transfers in euros provides uniform rules for cross-border IPs in euros to increase adoption of IPs and open banking. It also includes provisions to manage fraud, money laundering, and sanctions related to IPs. Tiered implementation was introduced, and the following implementation dates remain for payment service providers (PSPs):

January 9, 2027

- PSPs based in a country whose main currency is not the euro shall offer payment service users (PSUs) the ability to send and receive instant credit transfers in euros.
- PSPs based in a country whose main currency is not the euro should offer IPs at no additional costs.

April 9, 2027

- PSPs that are electronic money institutions or payment institutions based in a country whose main currency is the euro shall offer PSUs the ability to send and receive IPs.
- PSPs that are electronic money institutions or payment institutions based in a country whose main currency is not the euro shall offer PSUs the ability to receive IPs.

July 9, 2027

- PSPs based in a country whose main currency is not the euro shall offer verification of the payee services.
- PSPs that are electronic money institutions or payment institutions based in a country whose main currency is not the euro shall offer PSUs the ability to send IPs.

Source: ComplyAdvantages' A Guide to Financial Crime and SEPA Instant Payments.

Crypto & stablecoins

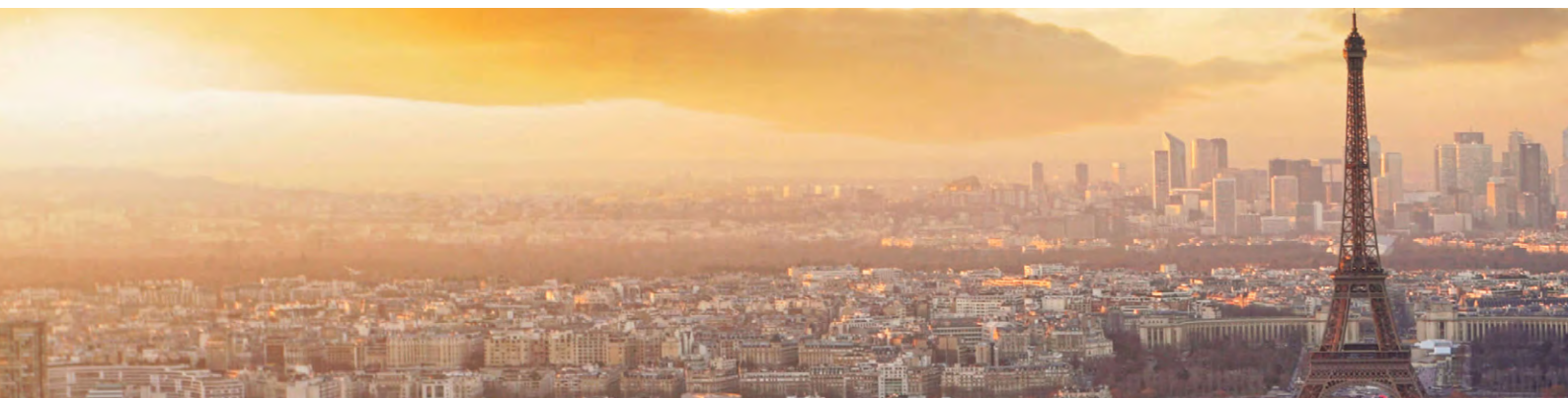
The EU will continue its rollout of Level 2 and Level 3 measures to implement the Markets in Crypto-Assets Regulation (MiCA). MiCA was issued as part of the EU's Digital Finance strategy to support the digital transformation of finance while mitigating risks. MiCA looks to apply uniform rules for crypto-asset issuers and crypto-asset service providers (CASPs) and create an authorization and supervision regime for stablecoins across the region. Stablecoins are defined as e-money tokens, or "crypto-assets that stabilize their value in relation to a single official currency," and asset-referenced tokens, or "crypto-assets that stabilize their value in relation to other assets or a basket of assets." It also required CASPs to have in place policies and procedures to prevent and detect ML and TF, and sets out rules to mitigate market abuse, including prohibitions on the disclosure of inside information, insider trading, and market manipulation. While CASPs have been subject to authorization for some time, grandfathering provisions for existing firms providing services end on July 1, 2026.

ESMA recently issued a table containing an overview of Level 2 (legally binding Regulatory Technical Standards [RTS] and Implementing Technical Standards [ITS]) and Level 3 (guidelines, opinions, and Q&As from European authorities) measures. This includes an opinion on the interplay between the *Payment Services Directive 2* (PSD2) and MiCA, a Q&A on the grandfathering clause and applicable AML laws, and guidelines for issuers to maintain systems and security access protocols to appropriate EU standards, amongst many other measures.

High-risk third countries

Firms operating in Europe should remain aware of any future updates to the list of high-risk third countries identified as having strategic deficiencies in their AML/CFT regimes. The list may be updated more than once per year. Higher-risk third countries include:

#	High-risk third country
1	Afghanistan
2	Algeria
3	Angola
4	Burkina Faso
5	Cameroon
6	Côte d'Ivoire
7	Democratic Republic of the Congo
8	Haiti
9	Kenya
10	Laos
11	Lebanon
12	Mali
13	Monaco
14	Mozambique
15	Myanmar
16	Namibia
17	Nepal
18	Nigeria
19	South Africa
20	South Sudan
21	Syria
22	Tanzania
23	Trinidad and Tobago
24	Vanuatu
25	Venezuela
26	Vietnam
27	Yemen



Enforcement

The European Commission (EC) will continue to take action against countries that fail to adopt measures to transpose EU sanctions-related directives into national law. The EC opened infringement procedures against 18 Member States for failing to criminalize the violation and/or circumvention of financial and economic sanctions through the implementation of the Criminal Offenses and Penalties for the Breach of EU Restrictive Measures.

The table below contains a list of additional enforcement actions taken by different jurisdictions in Europe:

Date	Amount (EUR)	Sector	Country	Description
Feb 17	120,000	Anonymous	Netherlands	Export of industrial equipment to occupied Crimea.
April 4	283,000	Investment management	Luxembourg	Breaches of anti-money laundering laws related to the company's due diligence procedures for both investors and intermediary investors.
July 1	600,000	Commercial banking	France	Failure to collect data on directors and owners for large number of businesses it served. Inadequate screening of transactions.
August 13	153,000	Investment banking	Iceland	Lack of adequate and ongoing screening.
September 3	214,000	FinTech	Luxembourg	Failure to file suspicious transaction reports in multiple cases of suspected counterfeiting.
September 8	100,000	Brokerage	Netherlands	Failure to complete sanctions compliance questionnaires.

France

Firms should ensure that they have updated internal suspicious transaction report/suspicious activity report (STR/SAR) filing processes to ensure that they are now compliant with the Decree laying down procedures for filing reports to TRACFIN, the French FIU, in line with Article L.561-15 of the Monetary and Financial Code. The Decree was issued to amend existing processes and procedures for filing STRs, thereby creating consistency across the reporting processes for all professionals subject to reporting requirements. Paragraphs III and IV of Article R561-31 of the Monetary and Financial Code detail the information that should be included in an STR and can now be submitted through the online platform, ERMES.

Crypto

The French government passed a law establishing a legal regime for the pledging of crypto-assets to allow them to be used as collateral, which is not covered by MiCA. Law No. 2025-391 is codified in the French Monetary and Financial Code. It includes rules on enforceability, publicity, and the right of pledges.

Germany

BaFin will likely begin assessing firms against the Interpretation and Application Guidance (AuA) of the German Federal Financial Supervisory Authority (BaFin) on the German Anti-Money Laundering Act (GwG). The revision requires firms to adopt a risk-based approach with senior management oversight; clearly distinguish between ML and TF risks; appoint a local MLRO; have enhanced identification and verification requirements; and clear timelines around ongoing monitoring of customer accounts. The German law also introduced EDD requirements for crypto transfers to or from self-hosted wallets (Section 15a GwG).

United Kingdom

The UK will continue to enhance its AML/CFT framework in the lead-up to its MER in 2027. HM Treasury is expected to publish a final version of the Money Laundering and Terrorist Financing (Amendment and Miscellaneous Provision) Regulations 2025, having recently published draft regulations alongside a policy note. The updated regulations aim to increase AML/CFT effectiveness, close loopholes, address concerns around proportionality, and take into account evolving ML and TF risks.

The revised draft regulations look to:

1. **Make customer due diligence "more proportionate and effective" by:**

- Aligning CDD requirements for letting agents, art market participants, and high-value dealers.
- Maintaining AML safeguards while facilitating continued access to banking services following bankruptcy and insolvency proceedings of a bank or building society.
- Ensuring that EDD is targeted, evidence-based, and proportionate. The regulations narrow the list of high-risk third countries to only those included in the FATF black list and clarify that EDD should be applied to "unusually complex or unusually large" transactions, measured against what is normal for the sector or type of transaction.
- Increasing supply and access of pooled client accounts (PCAs) for businesses with a legitimate need by removing the requirement to treat PCAs as low risk and introducing a requirement to take "reasonable measures" to understand the purpose of a PCA, the nature of the customer's business, and to carry out a risk assessment. To limit the need to carry out CDD on all customers while maintaining transparency, a new requirement has been introduced for those who hold PCAs to be able to provide banks with identity information held upon request.
- Requiring crypto-asset providers and custodian wallet providers to apply EDD in correspondent-type relationships and prohibiting relationships with shell banks.

2. **Strengthen system-level coordination amongst supervisors (including Companies House) and information sharing.**

3. **Clarify scope and issues around AML/CFT regulation by:**

- Converting thresholds to sterling (£10,000) to limit currency conversions to simplify compliance.
- Regulate the sale of off-the-shelf companies by trust and company service providers (TCSPs).
- Update registration requirements for crypto businesses, including adding a fit and proper test for controllers, whenever there are changes in control and beneficial ownership.

4. **Expand the categories of trusts that must register with the Trust Registration Service and introduce beneficial ownership requirements and exclusions for low-value, low-risk, or inappropriate trusts or trusts that deal with the administration of estates.**

The government has also committed to enhancing sector-specific AML/CFT guidance and to publishing additional guidance on the use of digital identity to meet CDD requirements.

The UK published its National Risk Assessment (NRA) in July 2025. Notably, there is a change in risk rating for specific sectors. The following sectors have been identified as being high risk for ML:

- Retail banking
- Wholesale banking and markets
- Wealth management
- Electronic money institutions (EMIs)
- Payment service providers (PSPs)
- Crypto-asset businesses
- MSBs
- Legal service providers
- Accountancy services
- TCSPs

Retail banking, EMI/PSPs, and MSBs have been classified as high-risk for TF. The NRA contains an overview of typologies, ML and TF threats, specific risks identified for regulated activities, and cross-cutting risks, including AI, schools and universities, and football clubs and agents. Businesses that have been reclassified as high-risk should review their AML/CFT systems and controls to ensure that they are able to manage their risks more effectively. Firms with clients in these industries should ensure that they apply a risk-based approach to understand their risk exposure, taking into account the types of products and services being offered, determine the level of due diligence and ongoing monitoring required, and tailor their own controls accordingly.

Crypto

As part of its proposal to create a regulatory regime for crypto-assets, including stablecoins, HMT issued a 'Future Financial Services Regulatory Regime' for cryptoassets (regulated activities) draft statutory instrument (SI) establishing the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) as regulators. The SI creates new categories of specified investments and definitions, including:

- "Qualifying cryptoassets," which are fungible and transferable.
- "Qualifying stablecoin," which is a stablecoin "that references one or more fiat currencies, and seeks to hold those fiat currencies or fiat currencies and other assets as backing assets to maintain a stable value.
- "Specified investment cryptoasset" which "is something that meets both the FSMA definition of a "cryptoasset" and the FSMA definition of a specified investment (for instance, an equity or a bond)," such as "a token on a blockchain that represents an interest in or right to an equity."

It also lists newly specified activities covered by the regulation. This includes the issuance of stablecoins, safeguarding (or "custody" of qualifying crypto-assets), operating a qualifying crypto-asset trading platform, dealing in crypto-assets lending and borrowing, dealing in crypto as an agent, arranging deals in qualifying crypto-assets, and qualifying crypto-asset staking. The SI also introduces a requirement for all crypto firms serving UK retail customers to be authorized to do so in the UK, amongst other measures.

Enforcement

The UK will continue to show credible deterrence through increased enforcement activity and fines. The UK's regulator, the FCA, issued a £39 million fine against a large financial institution for failing to identify, assess, monitor, and adequately manage money laundering risks associated with its corporate banking arm.

Asia

China

Firms can expect to see increased enforcement action by the People's Bank of China (PBoC) as the revised AML Law, which became effective on January 1, 2025, takes hold. The law introduced a number of changes. It expanded the scope of AML/CFT measures to include specific non-financial institutions, such as:

- Real estate developers and intermediaries
- Accounting firms
- Law firms
- Notary offices involved in real estate transactions
- Fund and securities management
- Client fundraising activities
- Dealers in precious metals and gemstones.

It introduced beneficial ownership requirements and a beneficial ownership registry, obligations for firms and individuals to comply with know your customer (KYC) measures, for firms to carry out customer due diligence (CDD), enhanced due diligence (EDD), and ongoing customer monitoring, and requirements for third-party service providers to risk assess parties carrying out due diligence on their behalf. The People's Bank of China (PBoC) issued a circular in 2025 requiring all cross-border e-commerce platforms to verify ultimate beneficial owners (UBOs) for merchants that have over RMB50,000 in sales.

Hong Kong

Hong Kong will continue to expand its digital finance footprint and promote information sharing to fight fraud. On May 25, 2025, the government introduced the Banking (Amendment) Bill 2025 to tackle fraud and related money laundering. The Hong Kong Monetary Authority (HKMA) found that nearly 44,800 fraud cases were reported, with victims losing HKD9.15 billion and facing "significant hardship and stress." The changes introduce private-to-private sector information sharing to cover individual accounts without consent.

On August 1, 2025, the government issued the Stablecoins Ordinance, creating a licensing regime for stablecoin users specifically as related to fiat-referenced stablecoins, making this a regulated activity under the HKMA.

HKMA has issued several related explanatory notes and guidelines:

- **July 2025:** Explanatory Note on Licensing of Stablecoin Issuers**,** which sets out the minimum criteria, application procedures, and ongoing obligations
- **July 2025:** Explanatory Note on Transitional Provisions for Pre-existing Stablecoin Issuers**,** including details of how to apply for transitional provisions, and details of transitional provisions for the first 3 months and the first 6 months
- **August 2025:** Guideline on Anti-Money Laundering and Counter Financing of Terrorism (For Licensed Stablecoin Issuers) **(AML/CFT Guideline),** which includes guidance on how to meet requirements around risk assessments, AML/CFT systems, CDD, ongoing monitoring, stablecoin transfers, TF, sanctions and PF, suspicious transaction reports, and record-keeping.
- **August 2025:** Guideline on Supervision of Licensed Stablecoin Issuers**,** which includes information on how to carry out activities linked to reserve asset management, issuance, redemption, and distribution of reserve assets, business activities, financial resources, including minimal capital requirements, risk management, and sound business practices and conduct.

With regards to enforcement action, HKMA took the following action against three banks in July 2025:

- A HK$8.5 million fine was issued for transaction monitoring failures and a lack of senior management oversight of the bank's AML/CFT controls. It was required to carry out a look-back review of past transactions and remediation activities to address identified deficiencies.
- A HK$4 million fine was issued for failing to include certain transaction types in the transaction monitoring system for ongoing monitoring.
- A HK$3.7 million fine was issued for transaction monitoring failings in a shared system.

Singapore

Singapore will continue to support global efforts to combat money laundering, terrorist financing, and proliferation financing, and will lead the way in promoting innovation in AML/CFT and taking regulatory action against financial institutions and senior managers responsible for AML/CFT programs. The Monetary Authority of Singapore (MAS) has signaled that it will share best practices to streamline processes and adopt AI and automation. Singapore's AML/CFT Industry Partnership (ACIP) also published a paper sharing industry best practice on counter proliferation financing.

In 2025, MAS published numerous Notices on the Prevention of ML/CFT. These set out specific regulatory requirements for different industry actors regarding risk assessment and risk mitigation, CDD, reliance on third parties, correspondent accounts and wire transfers, record-keeping, reporting of suspicious transactions, and internal policies, compliance, audit, and training. Notices were issued in June for the following regulated actors:

- Life insurers
- Trust companies
- Approved trustees
- Capital market intermediaries
- The Depository
- Approved exchanges and recognised market operators
- Financial advisers
- Exempt payment service providers
- Persons providing account issuance services who are exempted
- Financial institutions dealing in precious stones and precious metals
- Credit card or charge card licensees
- Digital payment token service
- Specified payment services
- Banks
- Trustee managers

For each updated notice, MAS also issued a number of supporting guidelines to allow different regulatory actors to comply with the issued notices that should be read together.

Regarding enforcement, MAS will continue to take action for AML/CFT and sanctions failures. In July 2025, MAS fined nine financial institutions, including major banks, two capital market services license holders, and a licensed trust company, a combined total of S$27.45 million for AML-related failures. These include:

Sector	Composition penalty
Banks	S$20.2 million
Capital market services license holders	S$5.25 million
Licensed trust companies	S$1.8 million

This includes failure to apply proper due diligence and monitoring measures linked to the customer risk assessment model; not establishing or validating source of wealth (SOW) when required; inadequate review of transaction monitoring alerts; application of insufficient or delayed risk mitigation measures (such as customer risk assessment review of enhanced monitoring) for customer accounts as post-suspicious transaction report follow-up. MAS also issued prohibition orders against individuals, including CEOs, Executive Directors, COOs, and Relationship Managers, for failing to ensure that AML/CFT systems and controls kept pace with business growth, failing to develop and implement adequate AML/CFT policies and controls across all AML/CFT requirements (SOW, customer risk assessments, screening, and ongoing due diligence), and failing to ensure controls were subject to regular audits.

Australia

Firms will need to comply with enhanced AML/CFT measures in Australia to mitigate and manage ML/TF risks and meet global best practice.

At long last, the implemented Tranche 2 reforms have been issued under the Anti-Money Laundering and Counter-Terrorism Financing Rules 2025 (the New AML Rules) and updated Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (the Act) and the Anti-Money Laundering and Counter-Terrorism Financing (Class Exemptions and Other Matters) Rules 2007 (Class Exemption Rules). Australia has opted for a staggered implementation with changes coming into effect as follows:

- March 31, 2026: AML/CFT changes apply to current reporting entities.
- March 31, 2026: Newly regulated Tranche 2 sectors must enroll with the Australian Transaction Reports and Analysis Center (AUSTRAC).
- July 1, 2026: Tranche 2 sectors must comply with AML/CFT measures.

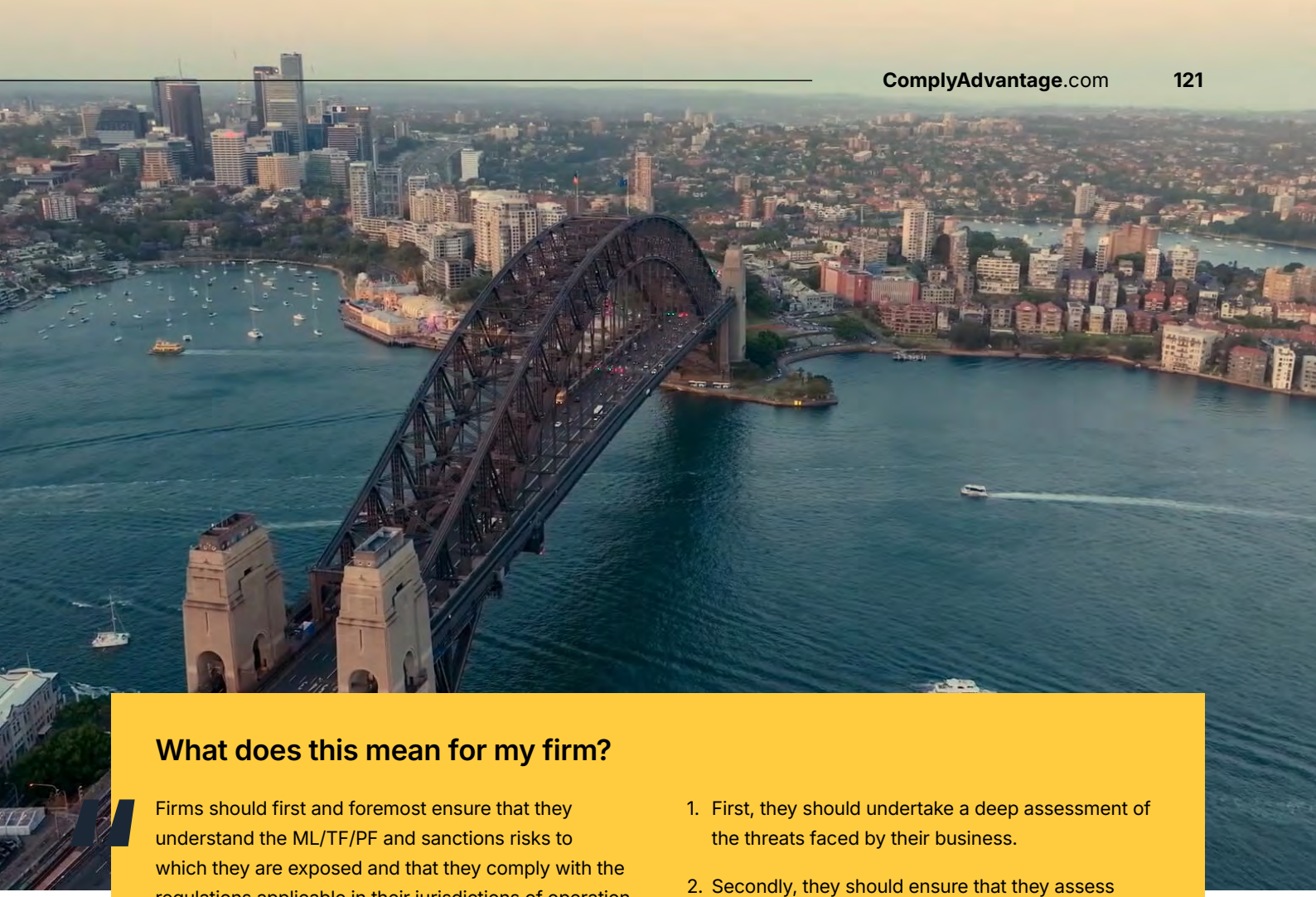
Changes require firms to draft an ML/TF risk assessment and identify if they offer any of the newly designated services. Additional updates include carrying out initial customer due diligence (ICDD), collecting a minimum amount of KYC information – including for persons acting on behalf of a customer, beneficiaries, and beneficial owners – and topping it up as required by the risk-based approach. It does not include "safe harbors" for sources deemed to be reliable and independent, and simplified due diligence requirements are softer.

They must also formalize policies and procedures, ensuring that staff roles and responsibilities are updated and that all relevant employees are appropriately trained. Tranche 2 sectors now covered by the rule include real estate, accounting, legal, trust and company services, precious metals and stones, and virtual assets.

Firms will also need to review supporting guidance developed by AUSTRAC. AUSTRAC has created a website with educational content, including a fact sheet for tranche 2 reporting entities, an AML/CFT Essentials Checklist, and webinars about national risk assessment for different regulated sectors, and reporting entity forum webinars.

AUSTRAC also set out its regulatory expectations and priorities for 2025-2026, focusing on quality reporting and the effective management of ML/TF/PF risks. Expectations listed for reporting entities include:

- Continue to implement current money laundering controls.
- Develop and document implementation plans that manage ML/TF/PF risks while transitioning policies, procedures, and systems to meet the obligations under the reformed AML/CTF Act.
- Show sustained effort and progress against implementation plans.
- Continue to manage ML/TF risks through the changes, including implementing any tactical improvements in the short term.
- Act now to review and strengthen existing frameworks, systems, and processes for managing ML/TF risks.



What does this mean for my firm?

Firms should first and foremost ensure that they understand the ML/TF/PF and sanctions risks to which they are exposed and that they comply with the regulations applicable in their jurisdictions of operation. As some countries move to deregulate or implement measures to simplify compliance, while others push forward with more robust regulations, firms should develop a strategy to enable them to monitor and embed changes. Given the flurry of activity in the AML/CFT space, firms need to ensure that they can monitor national changes in their countries of operation and where they offer services. As a general rule, the policies and procedures of firms should follow Head Office policy, or where local requirements are more stringent, top up local policy to meet local requirements. Adopting a higher policy standard than the minimum legal requirement is advisable, providing a more robust framework for interpreting complex or ambiguous edge cases. This applies to all aspects of AML/CFT/CPF programs, including business-wide risk assessments, customer and product risk assessments, CDD and ongoing monitoring, screening and payment filtering, training, reporting, record-keeping, and assurance processes. Firms should review local guidance and any AML/CFT fines issued to understand key areas of focus for regulators.

Local firms newly in scope of AML/CFT regulation in different jurisdictions should develop their internal AML/CFT frameworks in line with requirements and supporting guidelines issued by national authorities.

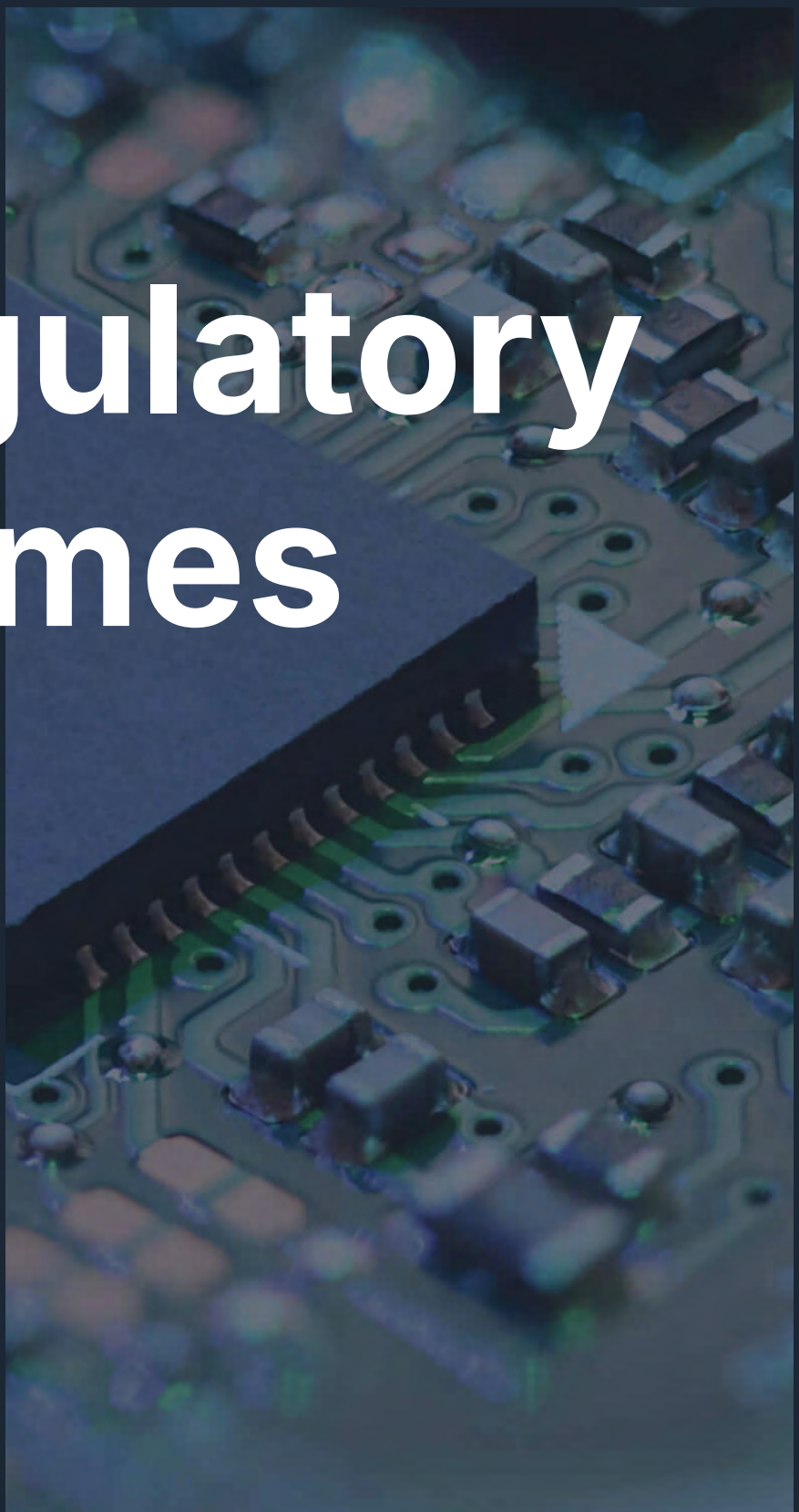
1. First, they should undertake a deep assessment of the threats faced by their business.
2. Secondly, they should ensure that they assess the level of ML/TF risk they face as a result of vulnerability to the identified threats.
3. Finally, firms should obtain the right level of support to ensure that they comply with requirements in a manner that is commensurate with the size, nature, and level of risk of their business and that they can execute the AML/CFT program on an ongoing basis.

If firms choose to outsource the development of AML/CFT policies and procedures, they should be aware that they retain corporate liability in most jurisdictions. Firms should review their off-the-shelf policies and procedures to ensure they are specific, relevant, and tailored to their unique needs. While some firms may consider using technology to support the development of policies and processes, firms should proceed with caution, given the degree of variance in local interpretations of AML/CFT laws and the risks associated with some emerging technologies. Firms should also consider the level of CDD/KYC measures for screening customers and relevant counterparties against adverse news and sanctions using a risk-based approach.

Iain Armstrong
Executive Director, FCC Strategy, ComplyAdvantage

Back to beginning
Previous section

Regulatory themes



Divergence in regulatory approaches

2026 will continue to see a divergence in regulatory practice. 2025 was a year marked by a push-and-pull dynamic: a trend toward global harmonization of standards and a concurrent divergence in approaches to and enforcement of AML/CFT among major players in this space. Although countries remain committed to the Financial Action Task Force (FATF) AML/CFT Standards, implementation varies widely, and changes in local law may lead to regulatory arbitrage and increased complexity for firms operating across borders. Key areas of divergence will include the level and intensity of supervision and enforcement.

Supervisory approaches

In Europe, a new era of harmonization and EU AML supervision began on July 1, 2025, with the establishment of a supranational supervisor, the Anti-Money Laundering Authority (AMLA). AMLA has been tasked with overseeing the coordination of national authorities and the enforcement of AML/CFT standards to foster a unified approach across the 27 member countries of the EU. The European Banking Authority (EBA) has recently identified that, while there has been an increase in regulatory engagement, with growing awareness of ML/TF risk, the effectiveness of AML/CFT systems and controls remains uneven. AMLA will transform AML/CFT supervision and enhance coordination among and between financial intelligence units (FIUs) to create a feedback loop, thereby strengthening enforcement and responses to ML/TF risks across the EU. AMLA will be issuing Level 2 and Level 3 rules and guidance to prepare all obliged entities across Europe for harmonized AML/CFT supervision. It is anticipated that beginning in 2026, AMLA will release:

1. Regulatory Technical Standards (RTSs) on lowering thresholds and identifying criteria for business relationships.
2. Guidelines for business-wide risk assessments.
3. Guidelines on ongoing monitoring of business relationships.

Another key shift is the move from a Directive-led to a Regulation-led regime in the EU. Whereas with Directives, countries are given a period of time to incorporate EU-wide requirements into national law, all obliged entities must comply with the AML/CFT Regulation when it becomes automatically applicable on July 1, 2027.

In contrast to the EU's push for centralization, the first half of 2025 saw a significant deregulatory shift in the US as part of the new administration's policy of "unleashing prosperity through deregulation." Effectively, 10 existing regulations need to be abolished to offset the cost of every new regulation that is drafted. To date, the US has limited the scope of the Corporate Transparency Act (CTA) to foreign reporting companies and has postponed final rules to address illicit finance risks associated with investment advisers and the real estate sector. The government has also assessed the costs of AML/CFT compliance with non-bank financial institutions (NBFIs), which is likely to lead to further deregulation. At the same time, however, the US has issued the first draft of the Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act, laying the foundations for the regulation of stablecoins.

> *One approach to navigating regulatory divergence is to look at all the markets where you have a presence, identify the highest standards, and then adopt a slightly higher standard still across the whole organization.*

Iain Armstrong
Executive Director, FCC Strategy, ComplyAdvantage

Hear more from Iain in our on-demand webinar: *AI innovation, new regulations, and evolving risks: What's in store for 2026?*

Enforcement

According to an analysis by Wolters Kluwer, the total volume of violations issued to financial firms fell by 37% in the first half of 2025 when compared to the preceding six-month period. Nevertheless, 2025 was a bumper year for enforcement with over $1.5 billion in AML fines.

AML fines	2024	2025	% change
Banking	$3.2 billion+ in fines	$200 million+ in fines	-94
Cryptocurrency	$86 million+ in fines	$1 billion+ in fines	+1063
Gambling	$86 million+ in fines	$22 million+ in fines	-74
Payments	$46 million+ in fines	$160 million+ in fines	+248
Trading and brokerage	$10 million+ in fines	$50 million+ in fines	+400

Divergence in approaches to enforcement is evident in the cryptocurrency space. Although one of the biggest fines in 2025 was issued against a crypto actor in the US (a large overseas exchange was fined $500 million for severe AML/CFT failings), President Trump issued a pardon against the founder of the world's largest crypto exchange, who had served jail time for money laundering violations. The US government also closed the federal inquiry linked to a criminal investigation of a founder of another exchange.

Regarding additional enforcement trends, there is a shift toward targeting digital payment service providers, FinTechs, and other non-traditional financial services firms. A digital payments firm was fined $40 million in the US for violating the Bank Secrecy Act (BSA), resulting from inadequate due diligence and transaction monitoring, which enabled it to open and maintain accounts associated with a Russian criminal network. The United Arab Emirates (UAE) issued the largest fine for AML/CFT failings against an exchange house for failing to trigger adequate levels of due diligence and transaction monitoring.

While supervisors continue to focus on traditional banking, the focus will likely shift to assessing the effectiveness of AML/CFT by FinTechs, which have been linked to prioritizing growth over compliance, and the crypto industry as it becomes increasingly regulated.

Across the EU, the EBA identified that most AML/CFT breaches related to customer due diligence (CDD) measures, including the failure to effectively apply CDD policies and procedures, errors in customer risk rating, ineffective ongoing monitoring, and weaknesses in customer identification and verification. The EBA further identified that poor implementation of RegTech is limiting the potential for stronger controls due to a lack of adequate in-house expertise, governance, and oversight in the deployment of RegTech solutions. Firms must also ensure that off-the-shelf solutions are fit for purpose. Additional failures identified on a global basis include sanctions violations, poor transaction monitoring, and improper suspicious activity report (SAR) filing.

What does this mean for my firm?

Firms will need to remain agile to respond to regulatory changes (including new changes and removal of requirements) as they emerge, with senior management and boards engaged early in understanding the materiality and implications of these changes. In addition to monitoring the regulatory landscape for ongoing developments, firms should identify any gaps and additional technology, skill sets, and resourcing needs, and forge a plan to update and roll out policies, processes, and systems. Firms should maintain an inventory documenting changes and ensure that they apply document governance and version control principles to key policy and procedural documents, thereby maintaining a clear audit trail of significant changes and senior management approvals. AML/CFT Officers will need to find a balance between regulatory expectations and internal demands within available budgets, leveraging best practices while maintaining oversight over any AML/CFT changes introduced to their firm. Firms operating across multiple jurisdictions will need to assess where regulatory approaches are converging versus diverging, and determine whether to maintain harmonized controls or implement jurisdiction-specific measures, balancing efficiency with regulatory appropriateness. Firms that have become subject to AML/CFT requirements should ensure that they obtain the right advice and tools to ensure they are relevant to their firm's risk profile and operating environment.

Regulatory change, while challenging, can serve as a catalyst for firms to modernize legacy systems, streamline inefficient processes, and enhance their overall financial crime risk management capabilities.

Iain Armstrong
Executive Director, FCC Strategy, ComplyAdvantage

Artificial intelligence (AI)

As AI becomes increasingly present in daily life and finance, regulators will continue to contend with the potential weaponization of AI. AI has emerged as a technology that can be used both to protect against and to perpetrate ML/TF and fraud at scale.

SHARE THIS

In the UK alone, investment scams increased by 55%, with an average loss of £15,000 per victim,

and romance fraud cases increased by 19%, with total losses estimated at £20.5 million. AI is also lowering the costs of committing personalized, culturally relevant fraud and scams, making low-value targets across borders increasingly attractive.

Fraud is now globally recognized as one of the key drivers of money laundering.

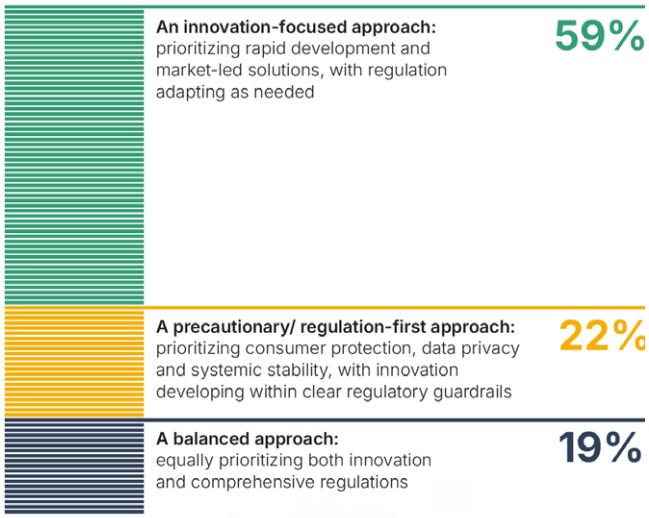
Conversely, both traditional and non-traditional financial firms are increasingly leveraging AI to intercept fraud and scams. This defensive shift is already yielding results, with banks successfully preventing £870 million in unauthorized fraud.

The financial crime industry is actively leveraging cutting-edge technology to combat these threats. Advanced AI and machine learning techniques, such as deep learning, social network analysis, and supervised/unsupervised models, are being applied to develop more robust AML/CFT controls.

These capabilities promise to automate core processes like know your customer (KYC), enhance suspicious activity detection, streamline investigations, and significantly reduce false positives. Furthermore, AI can be used to automate regulatory reporting, enhance risk scoring, and auto-remediate Level 1 alerts. The anticipated benefits of this AI adoption are substantial, including increased efficiency, improved predictive accuracy, faster resolution times, and lower operational costs in the long term. This technology shift is occurring within a rapidly expanding market, projected by the United Nations to reach $4.8 trillion by 2033.

On a global level, governments have called for responsible, trustworthy, human-centric, explainable, secure AI. And while the regulation of AI remains in its infancy around the world, there are emerging areas of concern that regulators will continue to focus on, seeking to strike a balance between the potential harms and benefits of AI while not stifling innovation. In our global survey, when asked about the most effective approach to AI regulation, the majority (59%) of senior financial crime professionals favored an innovation-focused approach, one that prioritizes rapid development and market-led solutions, with regulation adapting as needed. This was significantly higher than those who preferred a precautionary/regulation-first approach (22%) or a balanced approach (19%).

Which approach to AI regulation do you personally perceive to be the most effective?



Source: ComplyAdvantage, The State of Financial Crime 2026

Only a handful of countries, including those in Europe, China (including Hong Kong), and Japan, have adopted laws to regulate AI.

Numerous countries are drafting legislation or have established voluntary codes to manage the risks associated with AI. The majority of legislation aims to promote transparency, explainability, fairness, governance, and accountability in order to address bias in algorithmic decision-making. Firms should also be aware that most countries have existing regulations that are not AI-specific, but which are relevant to managing AI risks associated with financial crime. This includes laws related to privacy and data protection, copyright, and online safety and security.

> *"At the end of the day, if you're a BSA officer or an AML officer [...] and you have the best transaction monitoring system in the world, but you can't explain how it works, you have already lost."*

Robin Garrison
CAMS-Audit, Managing Consultant, Bates Group

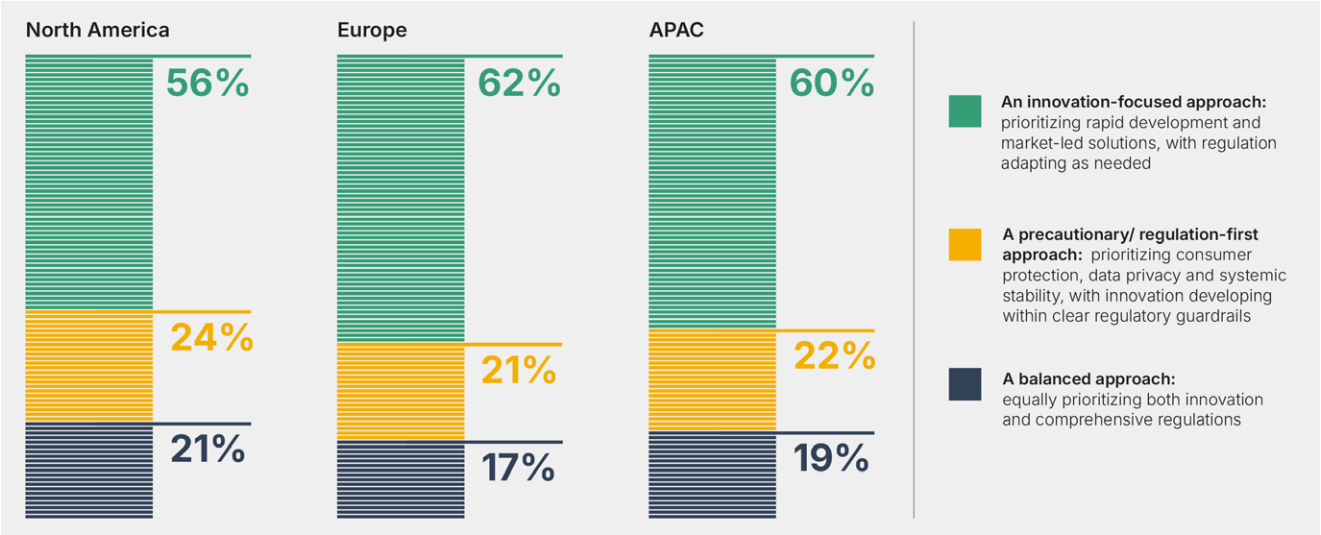
Hear more from Robin in our on-demand webinar: *AI regulation and the future of AML: Navigating compliance in a changing landscape*

On a global level, China, the US, and the United Arab Emirates (UAE) are competing to become the global leader in AI, while other countries are introducing measures to develop AI in a human-centric and responsible manner. China has led the way in regulating AI with its first AI strategy published in 2017, stating it would become a global leader in AI by 2030. Various laws and regulations governing AI adoption have been enacted since. China now requires firms to comply with the new 'Labelling Rules,' which require AI-generated content to be clearly labeled. The US's Executive Order 14179 on "removing barriers to American leadership in artificial intelligence" was issued on January 23 to make the US the global leader in AI and to revoke AI policies seen as barriers to innovation under the Biden administration. At the same time, states are moving forward in developing their own state-level legislation to address high-risk AI, consumer protection, algorithmic bias, the use of bots, and automated decision systems for employees. The UAE is poised to become one of the key testing grounds for AI, with plans to make Abu Dhabi the "world's first native AI-powered government by 2027" with significant investment in this space.

In Europe, the EU's AI Act, which forms part of its AI Innovation Package and Coordination Plan on AI, was drafted to "guarantee the safety and fundamental rights of people and businesses when it comes to AI," including democracy and the rule of law. The recently issued EU General-Purpose AI Code of Practice will support compliance with the legal requirements on safety, transparency, and copyright of general AI models, in line with the AI Act. The AI Act has been phased in throughout 2025, with its requirements fully applying by August 1, 2026. The Code is complemented by guidelines on the scope of obligations for providers of general-purpose AI models under the AI Act.

These divergent regional regulatory stances appear to be influencing firm sentiment. For example, while the US and Canada enjoy a less prescriptive AI regulatory environment, North American respondents of our survey were the least inclined to favor an innovation-led approach (56% support), contrasting with 62% in EMEA and 60% in APAC. Conversely, North America showed the highest combined preference for a balanced approach (21%) or a regulation-first approach (24%). This suggests that firms operating in environments with less prescriptive regulation may actually feel more exposed to the risks of new AI models. Lacking clear governmental guardrails, North American firms appear to be signaling a greater need for clarity and structured guidance on AI explainability, governance, and safeguards.

Which approach to AI regulation do you personally perceive to be the most effective? (Geographic breakdown)



Source: ComplyAdvantage, The State of Financial Crime 2026

In the EU and the UK, regulatory sandboxes continue to be set up to foster innovation in a safe and controlled testing environment.

The UK has launched the AI Opportunities Action Plan as a roadmap to accelerate AI adoption and put forward the Artificial Intelligence (Regulation) Bill, which calls for the creation of an AI Authority, regulatory sandboxes, AI responsible officers posts within AI firms, and transparency, IP, and labelling obligations. The Bill will continue to go through the legislative consultation and adoption process in 2026.

> *The conversation has evolved from a position of skeptical hesitation to one where regulators are becoming 'enablers,' recognizing that AI adoption is necessary for producing positive customer outcomes and enhancing the stability of the financial system overall.*

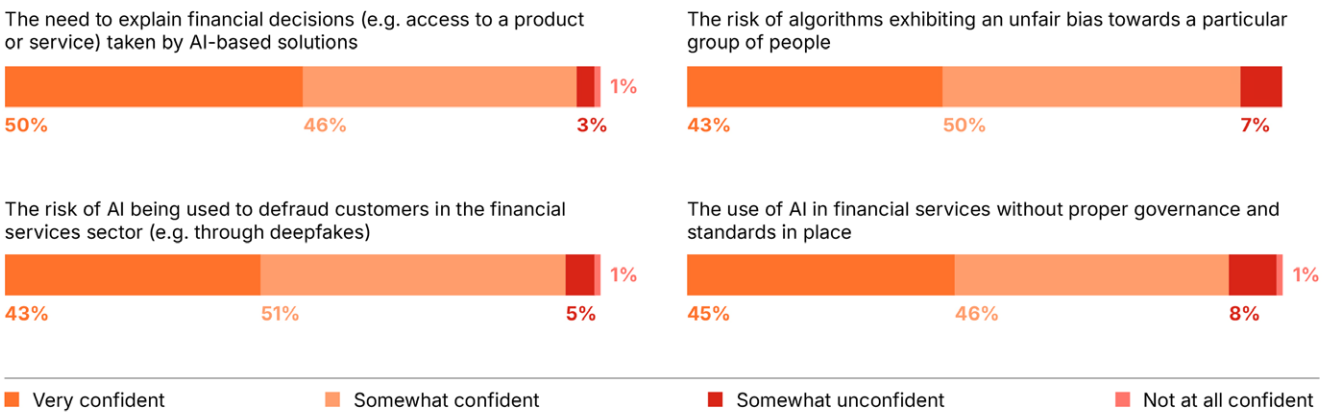
Annegret Funke
Financial Crime Senior Manager, PwC

Hear more from Annegret in our on-demand industry panel session from CATALYST 2025

Against this patchwork of emerging AI regulation, firms are actively evaluating their readiness and the effectiveness of legislative efforts in mitigating core risks. When asked, "How confident do you feel that the existing and proposed AI regulations in your jurisdiction will effectively mitigate the following risks posed by AI?", our 600 respondents expressed high confidence that existing and proposed AI regulations will effectively mitigate key risks:

- **Risk of AI being used to defraud customers:** 94% (43% very confident, 51% somewhat confident) were confident that regulation will address the risk of AI being used to defraud customers (e.g., through deepfakes).
- **Need to explain financial decisions:** 96% (50% very confident, 46% somewhat confident) were confident in regulations mitigating the need to explain financial decisions taken by AI-based solutions.
- **Use of AI without proper governance:** 92% (46% very confident, 46% somewhat confident) were confident in regulations addressing the use of AI in financial services without proper governance and standards in place.
- **Risk of unfair bias:** 93% (43% very confident, 50% somewhat confident) were confident that regulation will address the risk of algorithms exhibiting an unfair bias towards a particular group of people.

How confident do you feel that the existing and proposed AI regulations in your jurisdiction will effectively mitigate the following risks posed by AI?

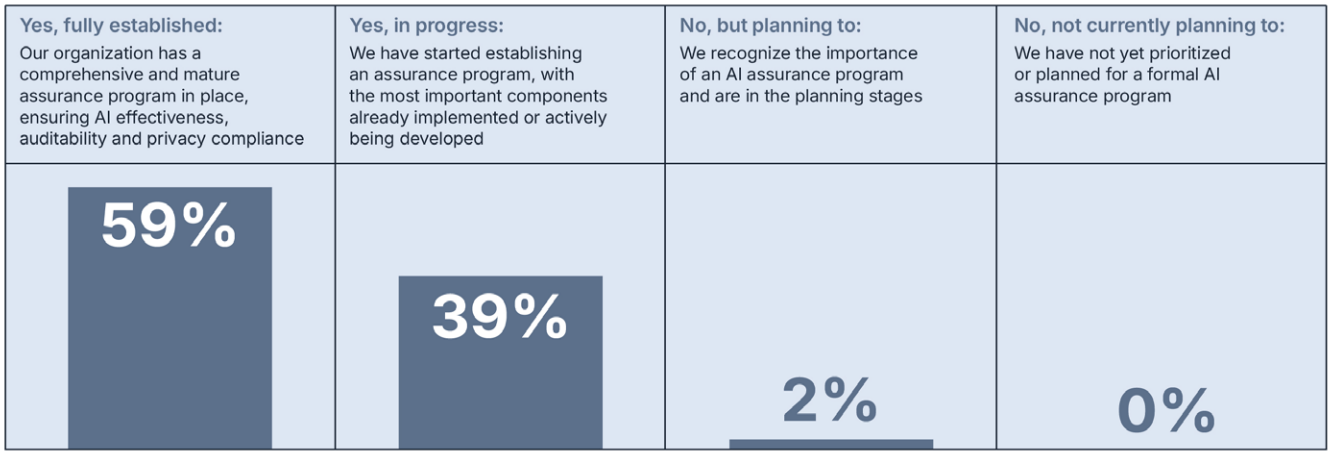


Source: ComplyAdvantage, The State of Financial Crime 2026

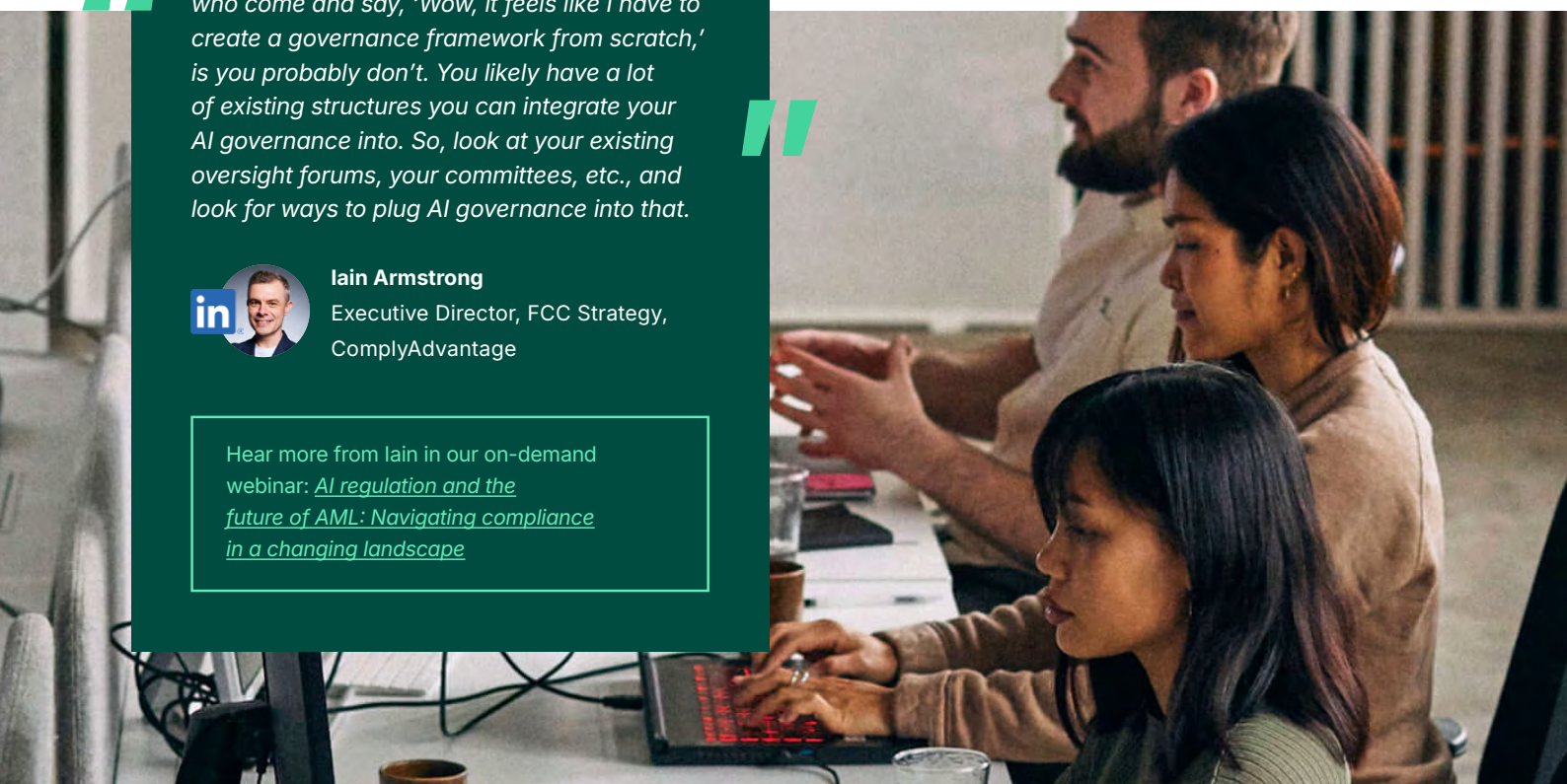
Furthermore, when asked, "Does your organization have an assurance program for AI to ensure its effectiveness, auditability, and adherence to privacy standards & model risk governance?", 98% of organizations stated they had a program in place or had started establishing one. The data shows that while commitment is high, implementation lags: our survey reveals that 41% of organizations have yet to fully establish or create a comprehensive AI assurance program. This means that while firms feel legislatively confident, a significant portion of the industry is still working to build the full governance and auditing structures needed to defend automated decisions and mitigate algorithmic bias.

However, despite the overwhelming confidence (94%) that regulations can mitigate AI-enabled fraud, the sheer pace of generative AI development raises a crucial question: Will current regulatory frameworks and proposed legislation be agile enough to keep pace with the evolving capabilities of large language models (LLMs) and other generative AI (GenAI) tools used in fraud and money laundering?

Does your organization have an assurance program for AI to ensure its effectiveness, auditability and adherence to privacy standards & model risk governance?



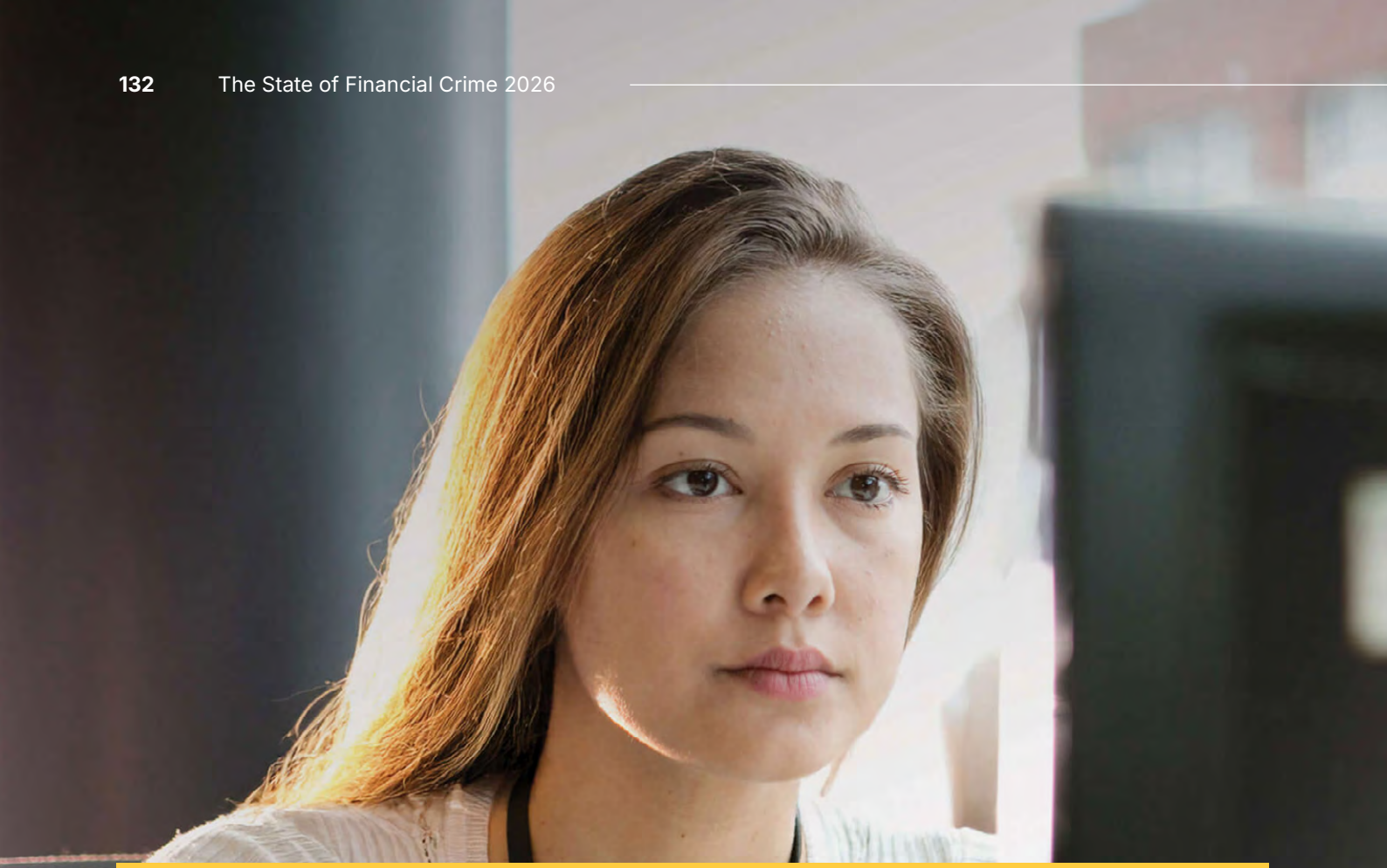
Source: ComplyAdvantage, The State of Financial Crime 2026



> *One thing I've been saying to a lot of our clients, who come and say, 'Wow, it feels like I have to create a governance framework from scratch,' is you probably don't. You likely have a lot of existing structures you can integrate your AI governance into. So, look at your existing oversight forums, your committees, etc., and look for ways to plug AI governance into that.*

Iain Armstrong
Executive Director, FCC Strategy, ComplyAdvantage

Hear more from Iain in our on-demand webinar: *AI regulation and the future of AML: Navigating compliance in a changing landscape*



What does this mean for my firm?

Firms should seek out the right level of expertise in AI regulation, governance, and risk management to identify and comply with applicable touchpoints between AI-enabled AML/CFT systems and controls, as well as relevant AI laws and standards, including data privacy and algorithmic decision-making.

Firms must actively manage the tension between their desire for innovation and the emerging regulatory patchwork. While the industry favors an innovation-first approach, the onus is on firms to establish their own stringent, auditable controls ahead of prescriptive governmental regulation, especially in jurisdictions where guidance is currently limited.

Although AI is seen as a beacon of efficiency and cost savings, firms must ensure that they understand the type of data used to train AI models, **explain how the model works**, and conduct robust testing when implementing an AI-enabled solution. Firms should also adopt a human-in-the-loop approach to identify and prevent algorithmic bias, and to review, validate, and explain automated decisions made to not offer accounts and products due to ML/TF concerns.

Firms should also consider adopting best practice around AI, including:

- Obtaining senior management support and documenting governance frameworks.
- Determining use cases and identifying data sources, data management processes, and internal systems needed to embed AI effectively.
- Carrying out risk assessments and developing risk management processes for AI.
- Carrying out vendor due diligence, including the level of experience in building AI models, the application of ethics, and the context in which AI models have been developed.
- Executing extensive model validation and bias prevention activities.
- Testing AI tools in a secure environment with appropriate safeguards.
- Carrying out ongoing monitoring and assurance.

Andrew Davies
Head of Global FCC Strategy, ComplyAdvantage

Stablecoins changing the real-time payments landscape

The stablecoin market has seen explosive growth, with transaction values surging by 54% in 2024 to reach $5.7 trillion, and the average supply of USD-backed stablecoins reaching $235 billion by mid-2025. In 12 months, stablecoins processed $9.8 trillion in transaction volume, and the stablecoin market is expected to grow to $2 trillion by 2028.

SHARE THIS

And while this pales in comparison to traditional payments, this growth has made stablecoins a key component of the future of payments.

Stablecoins offer a faster and more cost-effective alternative to traditional payments,

emerging as a solution for use cases such as financial inclusion, cross-border payments, and remittances, among others.

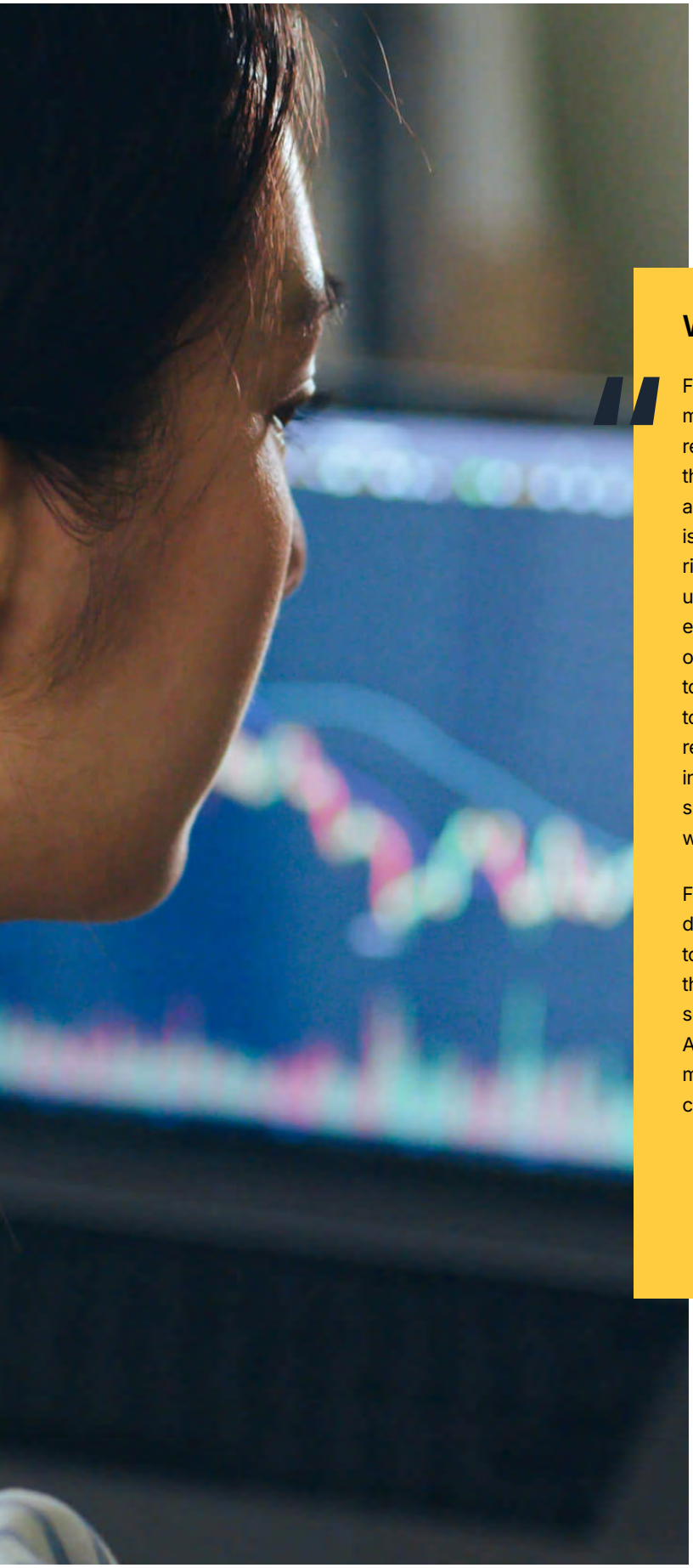
Stablecoins also offer a stable value when compared to highly volatile currencies, improve transparency (making it easier to monitor currency reporting requirements), and expand the set of payment options for consumers.

There is a push on a worldwide basis to introduce stablecoin regulation to address consumer protection issues that were brought to light with the collapse of Terra/Luna, which resulted in billions of dollars in losses for unqualified investors, including vulnerable communities, many of whom lost their savings and pensions. Japan was the first country to issue stablecoin regulation in 2022, closely followed by the EU and, more recently, Hong Kong and the US. In Japan, stablecoins can only be issued by banks, trust companies, and licensed money transfer agents. The EU's Markets in Crypto Assets (MiCA) Regulation extends traditional compliance requirements, including governance, consumer protection, consumer education, marketing, market integrity, market abuse, and AML/CFT measures, to stablecoins. All issuers of stablecoins in and/or offering services in Europe will be required to comply with MiCA and AML/CFT requirements by 1 July 2026. The Stablecoins Ordinance in Hong Kong introduced a licensing regime for stablecoins and an offense for fraud and deception punishable with a fine of between HK$1 million and HK$10 million and between 3 and 10 years' jail time. Recently, Hong Kong issued a Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Stablecoin Issuers) in August 2025. There is also a push to regulate stablecoins in support of the growth agenda.

The US GENIUS Act was fast-tracked and signed into law on July 18, 2025, to "pave the way for the United States to lead the global digital currency revolution" and "make America the crypto capital of the world." The Act establishes a Federal regulatory system for stablecoins, requiring 100% reserves and mandatory reserve holdings disclosures. It introduces marketing rules to protect consumers from "deceptive practices" and aligns State and Federal frameworks on stablecoins to ensure consistency.

In addition to addressing de-dollarization by driving demand for the US dollar as the global reserve currency for stablecoins, the US has also extended the BSA to stablecoins to combat illicit activities. Notably, stablecoin issuers are required to possess the technical capability to seize, freeze, and burn stablecoins when legally mandated. US stablecoins account for 99% of the global stablecoin supply.

Across APAC, stablecoin adoption is accelerating as regulators seek to balance consumer protection and illicit finance risks with innovation and growth. The APAC region is the fastest-growing in terms of on-chain value received for crypto, increasing from $81 billion in July 2022 to $244 billion by December 2024, with on-chain value consistently exceeding $185 billion per month throughout 2025. In India, stablecoins are being utilized for remittances, with digital payment infrastructures like UPI and eRupi facilitating their adoption. South Korea's market share is growing, with stablecoins used by traders to manage liquidity, hedge against market movements, and facilitate asset transfers. KRW-denominated stablecoins account for just over 80% of stablecoins purchased in APAC, amounting to about $65 billion. The Bank of Korea warned private issuers of the de-pegging risks associated with stablecoins and called on traditional banks to take the lead in issuing won-backed stablecoins. In Vietnam, stablecoins are used for remittances and savings, and in Pakistan, stablecoins are used to hedge against inflation. In October 2025, Japan issued the world's first yen-pegged stablecoin, the JPYC, which is fully convertible to the yen and backed by Japanese government bonds and domestic savings. The company, start-up JPYC, announced that it would issue 10 trillion yen ($66 billion) of JPYC over three years. Japan's three largest banks, Mitsubishi UFJ Financial Group (MUFG), Sumitomo Mitsui Banking Corp., and Mizuho Bank, are also expected to issue a joint stablecoin for their corporate clients. China is also considering issuing yuan-backed stablecoins to promote global adoption of its currency as Chinese exporters increasingly use USD-backed stablecoins. Hong Kong's Stablecoin Ordinance, which became effective on August 1, 2025, could strengthen its ability to issue an offshore yuan stablecoin, and both Hong Kong and Shanghai have been cited as key cities to boost the development of a yuan stablecoin. Australia has stated its intention to develop an innovative digital asset industry, including a framework for payment stablecoins, which will be treated as a type of stored value facility (SVF).



What does this mean for my firm?

Firms considering expanding into the stablecoin market should ensure they become familiar with the requirements surrounding stablecoins, particularly if they plan to issue stablecoins, including compliance and AML/CFT requirements related to stablecoin issuance. Firms should explore developing a risk tolerance statement regarding stablecoins, understand the different types of stablecoins that exist, and manage not only AML/CFT but also operational and fraud risk exposures. Firms will need to understand the ML/TF risks posed by stablecoins to their businesses, including capital reserve requirements, the information that must be included in white papers, and the controls and measures that should be enhanced to mitigate the risks associated with working with stablecoins.

Firms should also consider developing a stablecoin due diligence questionnaire if providing services to stablecoin issuers. Lastly, firms looking to enter the stablecoin space should explore technology solutions to support them in developing their AML/CFT frameworks, including blockchain monitoring tools, due diligence, and Travel Rule compliance solutions.

Iain Armstrong
Executive Director, FCC Strategy, ComplyAdvantage

The public-private imperative

The FATF's Private Sector Collaborative (PSC) Forum will continue to shape public-private sector collaboration in the fight against financial crime. The 2025 PSC Forum underscored the vital role of public-private partnerships (PPPs) in strengthening global defenses against financial crime, with FATF President Elisa de Anda Madrazo stating: "The private sector is at the forefront of the fight against financial crimes. In this fight, public authorities and the private sector play on the same team." Public-private partnerships (PPPs) have long been recognized as critical to support information and financial intelligence sharing to prevent and detect illicit financial flows, stepping up "global defenses against financial crime." PPPs bring together representatives from not only banks and traditional finance firms, but also crypto exchanges, FinTechs, members of civil society, and designated non-financial businesses and professions (DNFBPs).

This drive for enhanced collaboration reflects a clear demand from the industry.

SHARE THIS

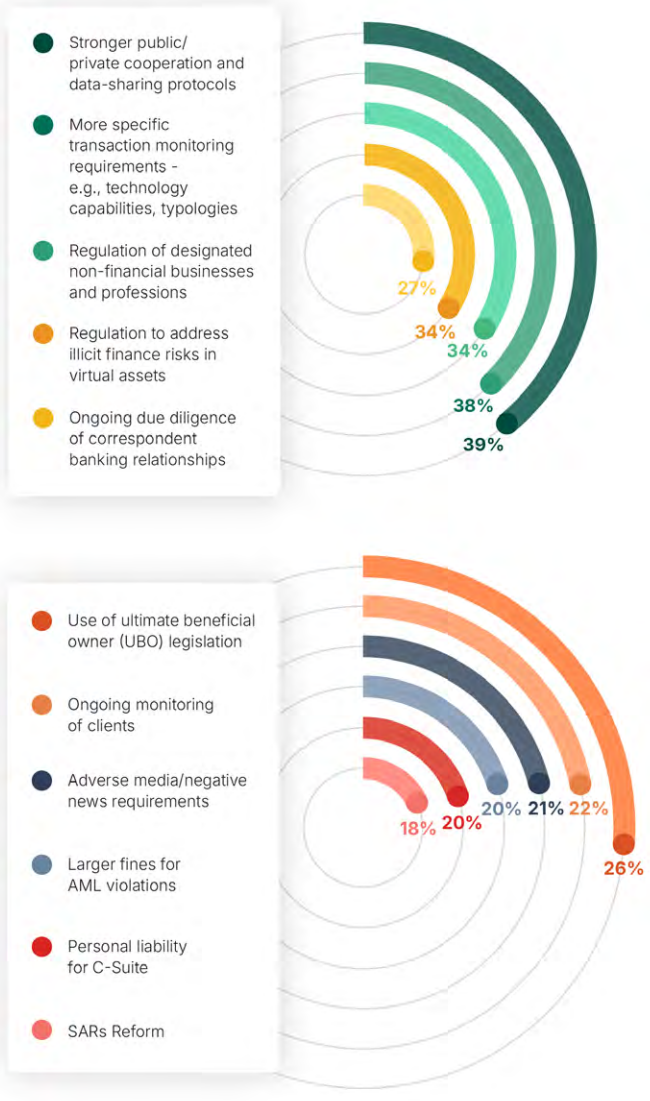
When we asked our respondents which areas of AML regulations required tightening in their country to have the greatest impact on financial crime,

"stronger public/private cooperation and data-sharing protocols"

topped the list at 39% (representing the share of respondents who ranked this option as one of their top three concerns).

This ranked slightly ahead of "More specific transaction monitoring requirements" (38%) and "Regulation of DNFBPs" (34%). The fact that greater public-private cooperation is seen as the single greatest regulatory lever available for impact suggests that firms feel constrained by current data-sharing limitations and view better information exchange as key to closing key defensive gaps.

Which areas of AML regulations require tightening in your country in order to have the greatest impact on financial crime?



Source: ComplyAdvantage, The State of Financial Crime 2026

Following last year's PSC Forum, the private sector will continue to refine the risk-based approach, including exploring how technology tools, such as digital customer onboarding, can support financial inclusion goals. Collaboration will continue on information sharing and data protection and privacy (DPP), including the use of privacy-enhancing technologies, through the new Forum on Data Frameworks, which was created to address inconsistencies in global data frameworks. The private sector will continue to inform revisions to Recommendation 16 (R16) and the 'Travel Rule,' which has evolved from a recommendation on wire transfer transparency to a recommendation on payment transparency, requiring firms to adopt tools to prevent fraud in payments.

Countries will continue to establish public-private intelligence sharing forums to facilitate information sharing through more direct channels, thereby increasing the quantity and quality of actionable intelligence. The UK's novel National Crime Agency (NCA) data sharing partnership will continue to see UK banks carrying out joint analysis with banking employees seconded to the NCA, working alongside NCA analysts. The initiative brings together targeted bank transaction data and crime-related datasets to identify real-time data insights to identify the misuse of the financial system and stop economic crime. Singapore's private sector initiative, the Collaborative Sharing of Money Laundering/Terrorism Financing (ML/TF) Information and Cases (COSMIC) platform, will continue to allow the sharing of red flags to prevent crime. COSMIC was co-developed between MAS and six of Singapore's largest banks and is "the first centralised digital platform to facilitate sharing of customer information among financial institutions (FIs) to combat money laundering (ML), terrorism financing (TF) and proliferation financing (PF) globally." COSMIC will continue to focus on:

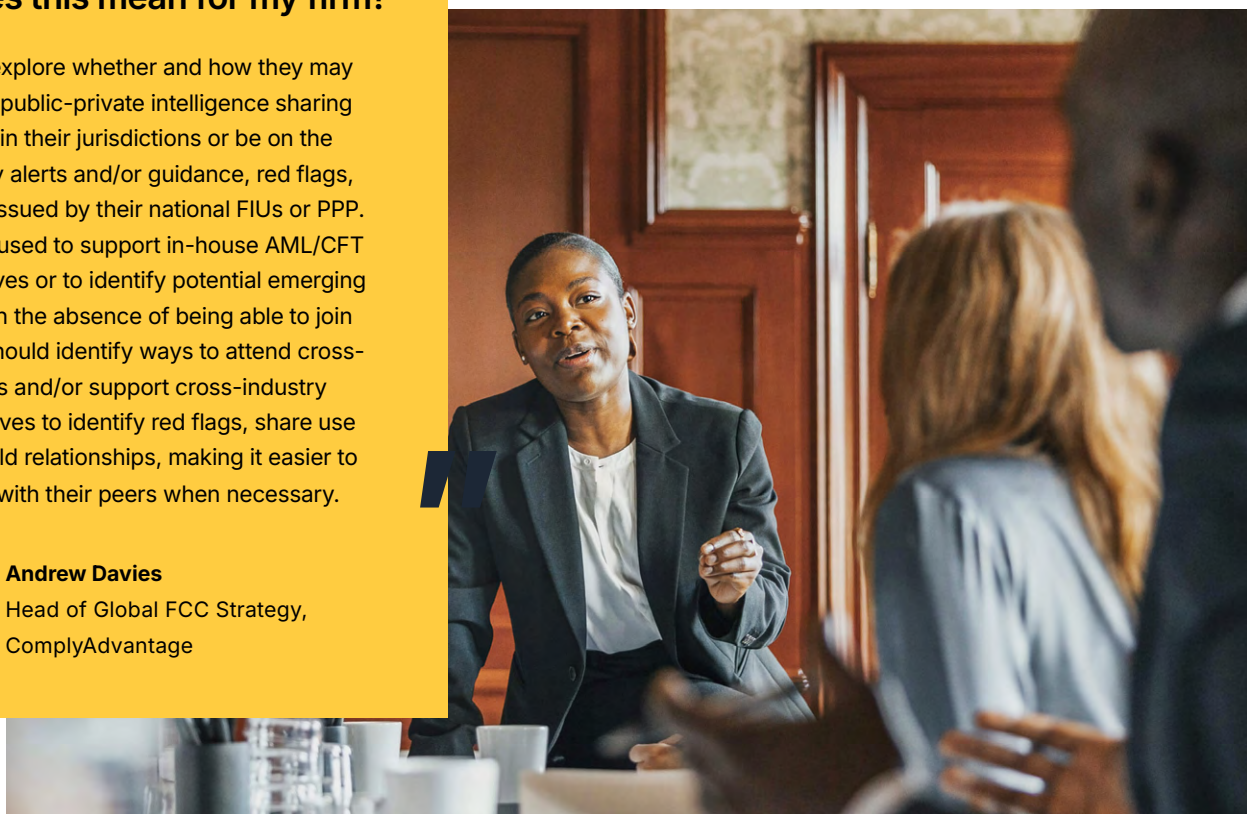
1. The misuse of legal persons.
2. The misuse of trade finance for illicit purposes.
3. Proliferation financing.

In 2026, there will be an increased shift to supporting private-to-private information and intelligence sharing to tackle fraud. The UK, Singapore, the EU, and Australia have all enacted legislation to support peer-to-peer information sharing in an effort to tackle illicit financial flows. The United Arab Emirates (UAE) and Hong Kong are expected to adopt similar laws. Meanwhile, the US and Mexico have introduced policy and operational changes to enhance collaboration on financial crime.

What does this mean for my firm?

Firms should explore whether and how they may be able to join public-private intelligence sharing arrangements in their jurisdictions or be on the lookout for any alerts and/or guidance, red flags, or typologies issued by their national FIUs or PPP. These can be used to support in-house AML/CFT training initiatives or to identify potential emerging areas of risk. In the absence of being able to join a PPP, firms should identify ways to attend cross-industry events and/or support cross-industry learning initiatives to identify red flags, share use cases, and build relationships, making it easier to communicate with their peers when necessary.

Andrew Davies
Head of Global FCC Strategy, ComplyAdvantage



Expanding the AML perimeter

The expansion of the AML perimeter beyond traditional financial institutions is a global trend. In Australia, the second tranche of reforms to the AML/CTF Act is underway, with significant compliance obligations set to commence on July 1, 2026, for real estate, accounting, legal, trust, and company services, as well as precious metals and stones, and virtual assets. Canada has recently extended AML/CFT requirements to factoring companies, cheque cashing businesses, and finance and leasing companies as part of the amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*. Mexico has brought Trusts, real estate developers, agents, and intermediaries that carry out "vulnerable activities," crypto exchanges, and virtual asset service providers (VASPs) within the scope of AML/CFT laws and regulations. In Europe, obliged entities now include crypto-asset service providers, crowdfunding platforms, certain types of intermediaries, professional football clubs and agents, dealers in precious stones and metals, dealers in high-value goods, and legal professionals facilitating certain higher-risk transactions, non-financial mixed activity holding companies, trust and company service providers, and investment migration operators. China's revised AML Law also extended AML/CFT measures to real estate developers and intermediaries, accounting firms, law firms, notary offices involved in real estate transactions, fund and securities management, and client fund-raising activity, as well as dealers in precious metals and gemstones.

In sharp contrast, the US will likely scale back AML/CFT measures due to cost considerations faced by NBFIs and will reassess whether AML/CFT measures should apply to investment advisers and individuals involved in real estate closings and settlements.

What does this mean for my firm?

As different sectors become subject to AML/CFT regulation, firms should assess the impact of regulatory requirements on customers who meet the new criteria in their books. This includes exploring whether this affects the level of risk associated with the customer and the application of simplified, standard, or enhanced due diligence. New firms subject to regulation should identify any guidance or guidelines issued by their regulatory or supervisory authority to understand how to implement new AML/CFT systems and controls. They should explore the types of tools and technologies required to manage AML/CFT risks and comply with new requirements. Lastly, firms should seek out advice when they lack in-house expertise on how to develop their AML/CFT programmes.

Andrew Davies
Head of Global FCC Strategy, ComplyAdvantage

About ComplyAdvantage

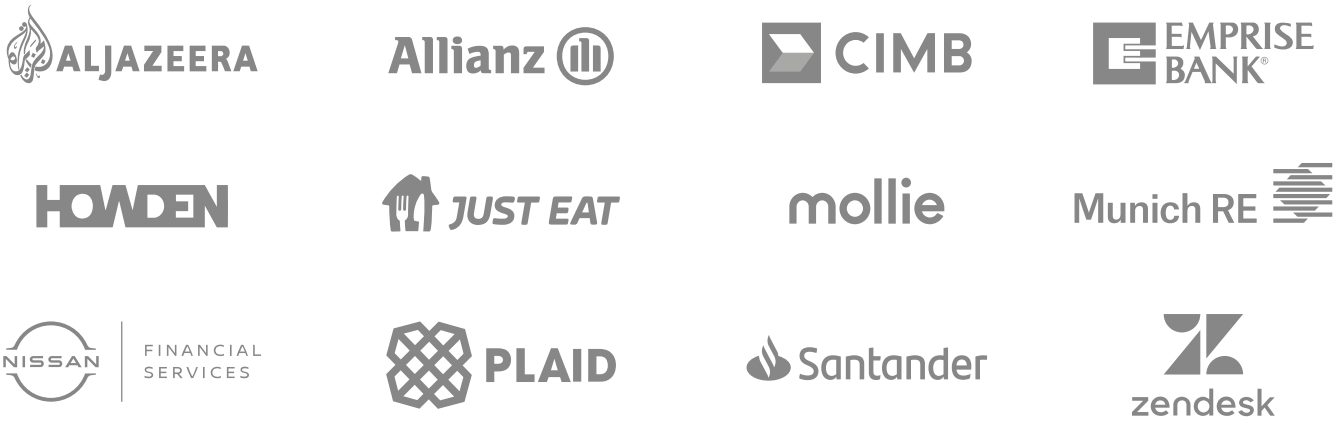
Our mission is to empower every business to eliminate financial crime.

By harnessing AI, a unified platform, and an extensive partner ecosystem, we help customers turn compliance into a catalyst for growth, operational resilience, and enduring regulatory trust.

More than 3,000 enterprises across 75 countries rely on our unified platform and the world's most comprehensive financial crime risk intelligence. With full-stack agentic automation, we help organizations automate up to 95% of KYC, AML, and sanctions reviews, cut onboarding times by 50%, reduce false positives by 70%, and handle 7x more work with the same staff.

ComplyAdvantage is headquartered in London and has global hubs in New York, Lisbon, Singapore, and Cluj-Napoca. It is backed by Balderton Capital, Index Ventures, Ontario Teachers' Pension Plan, Goldman Sachs, and Andreessen Horowitz. Learn more about compliance re-engineered for the age of AI at complyadvantage.com

Our customers



Get in touch

Sales

Interested in ComplyAdvantage's software? Fill out the form and our sales team will be in touch.

Speak to sales →

Partners

To connect with the partnership team, complete the Partner Program form.

Become a partner →

Press

For press inquiries please email us at press@complyadvantage.com.

Contact press →

Survey methodology

The State of Financial Crime 2026 is based on a survey of 600 C-suite and senior compliance decision-makers across the US, Canada, UK, France, Singapore, and Australia.

All respondents currently work in financial services and FinTech organizations, with 50+ employees and total assets worth $50 million+.

The sectors covered in interviews include financial institutions across payments, banking, and insurance.

COMPLY ADVANTAGE®

ComplyAdvantage.com

2026