COMPLY ADVANTAGE®

ComplyAdvantage.com

THE

State of Financial Crime

2025

COMPLY ADVANTAGE®

Contents

01.

Spotlight on financial crime

02.

Geopolitics and sanctions

03.

Regional regulatory trends

04.

Regulatory themes

Introduction

Welcome to the fifth edition of The State of Financial Crime, where we examine the evolving landscape of compliance, financial crime prevention, and regulatory change.

2024 was a year marked by escalating geopolitical tensions, with over 40 global elections driving an increased focus on politically exposed persons (PEP) screening and more stringent regulatory demands for transparency. Meanwhile, the rapid advancement of technologies like generative AI added new layers of complexity, as both compliance teams and fraudsters adopted these tools, further complicating the fight against financial crime.

Throughout the year, emerging risks and shifting compliance priorities put added pressure on firms to adapt. Geopolitical instability in Eastern Europe and the Middle East created fresh challenges, while persistent issues like siloed data continued to hinder effective risk management – nearly half of our survey respondents told us these data silos were a major obstacle, limiting their ability to detect and prevent financial crime and highlighting the urgent need for more cohesive data strategies.

On the regulatory front, the EU's Anti-Money Laundering Authority (AMLA) advanced efforts to harmonize AML regulations across member states. In the US, updates to the Corporate Transparency Act (CTA) and the Bank Secrecy Act (BSA) imposed enhanced scrutiny, particularly around beneficial ownership. Meanwhile, Singapore introduced tighter regulations under the Anti-Money Laundering and Other Matters Act, requiring banks, real estate firms, and digital payment providers to implement enhanced due diligence, ongoing monitoring, and new frameworks to address fraud and environmental crime-related money laundering.

At the same time, the global push for real-time payments, exemplified by the expansion of the EU SEPA Instant Credit Transfer (ICT) system, prompted firms to rethink their technology infrastructures to meet evolving requirements, often to the point of significant or complete overhaul.

Our survey results offer a glimpse into how organizations are adapting to these evolving dynamics. By providing these insights, we aim to help you benchmark your strategies, ensuring your organization remains resilient and proactive in the face of emerging challenges. With each year, the tools, resources, and guidance available to us continue to improve, empowering every financial crime fighter to stay one step ahead. Together, through our collective efforts and smarter strategies, we're not just fighting financial crime – we're helping create a safer, more transparent world for everyone.

We hope you enjoy reading this report as much as we've enjoyed compiling it.

Best,

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

Back to beginning

Next section

Spotlight on financial crime

The rising cost of compliance

2024 has been another mixed year for the global economy. In July, the United Nations Conference on Trade and Development (UNCTAD) forecasted an annual global growth rate of around 3 percent for the year – an improvement on the 2.2 percent of 2023 but still below pre-pandemic rates. McKinsey's Global Banking Annual Review for 2024 saw a similar pattern facing the financial services sector, noting that while 2022 and 2023 had been the best years for the industry since the global economic crisis in 2007-9, there remained "lingering market doubts over its long-term value creation potential." Much of the performance improvement had come from the sector's reliance on high interest rates to drive profits and increasing competition in areas such as payment services. Meanwhile, labor productivity challenges and regulatory reforms continue to push up costs, especially concerning internal investment in technology.

The unsettled environment has also had a knock-on effect on the world of compliance. PwC's EMEA AML Survey 2024, published in April, found that of the firms surveyed, 51 percent had seen compliance costs rise by over 10 percent in 2022 and 2023. Overall AML costs were up by an average of 14 percent, with staffing and technology the key factors. 55 percent of those surveyed by PwC also said they would invest more than 10 percent over the next two years. While the causes of this ongoing rise were, as with the rest of the sector, driven by market and regulatory concerns, other factors shaped compliance requirements. Global economic and financial crime was becoming increasingly sophisticated and broad in range as transnational organized crime groups took advantage of new technologies and a febrile geopolitical environment. The world will become even more dangerous and fragmented in 2024, creating gaps and opportunities for criminals to thrive.

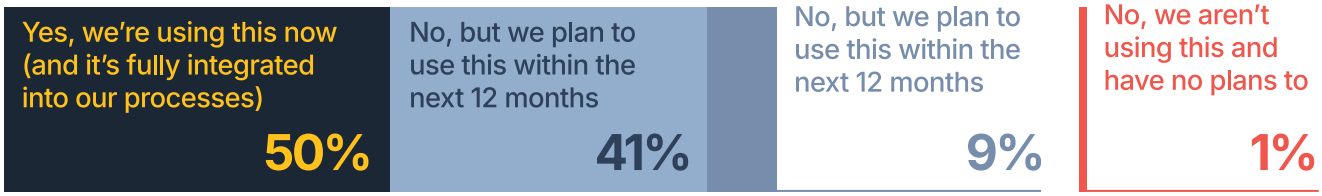
51% of firms surveyed saw compliance costs rise by over 10% in 2022 and 2023.

On a more optimistic note for financial services and compliance, however, 2024 also saw regulatory technology (RegTech) continue to progress, with ever more firms looking to advanced, cloud-based solutions that use machine learning and other forms of AI to improve the strength and resilience of their tech stack.

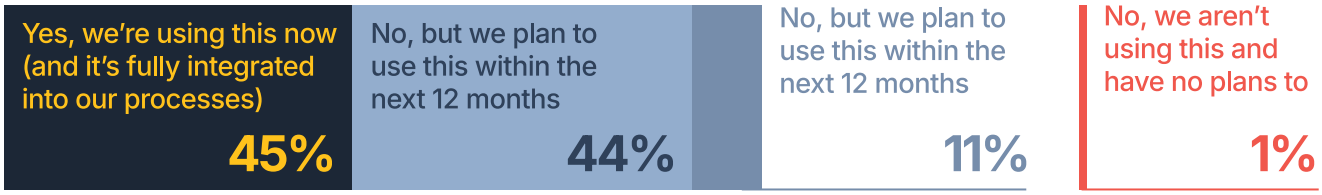
This trend seems likely to continue into 2025 and beyond. Our 2025 survey of global compliance decision-makers shows the growing adoption of AI-based technologies across various use cases, including alert prioritization, reducing remediation times, analyzing historical data, and creating reports using generative AI (GenAI).

How, if at all, is your organization using or intending to use artificial intelligence within the compliance function?

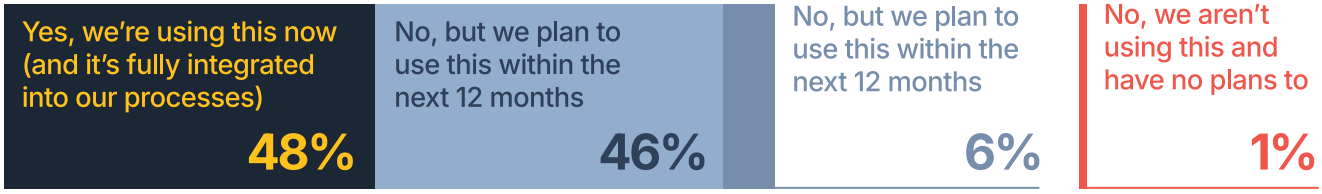
Prioritizing transaction monitoring alerts



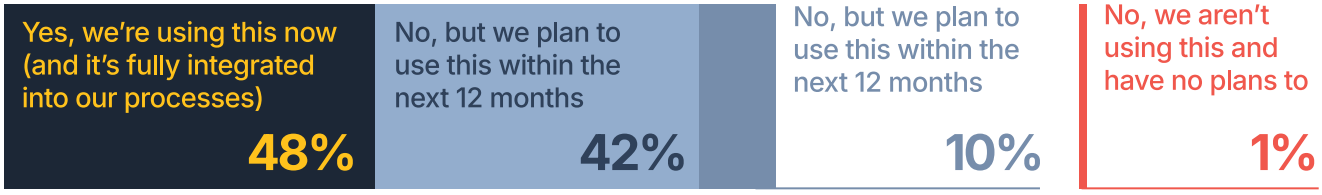
Reducing remediation times



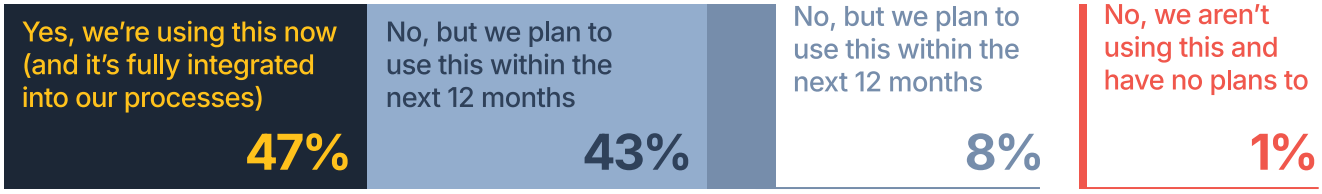
Analyzing historical transaction data



Forecasting future risks or patterns of risk



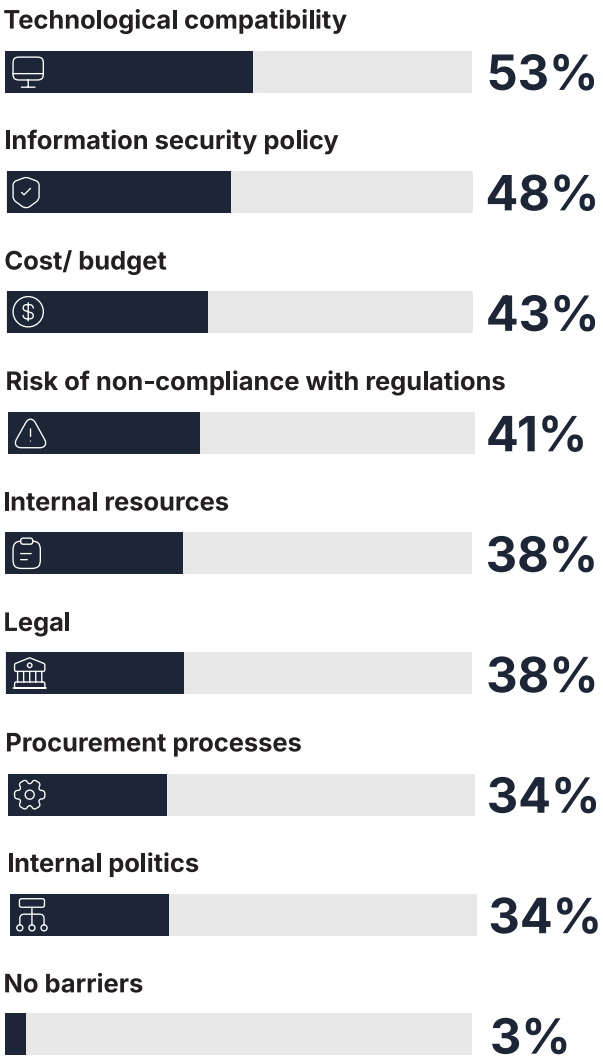
Generating reports (e.g. SARs) using copywriting tools such as ChatGPT



Source: ComplyAdvantage, The State of Financial Crime 2025

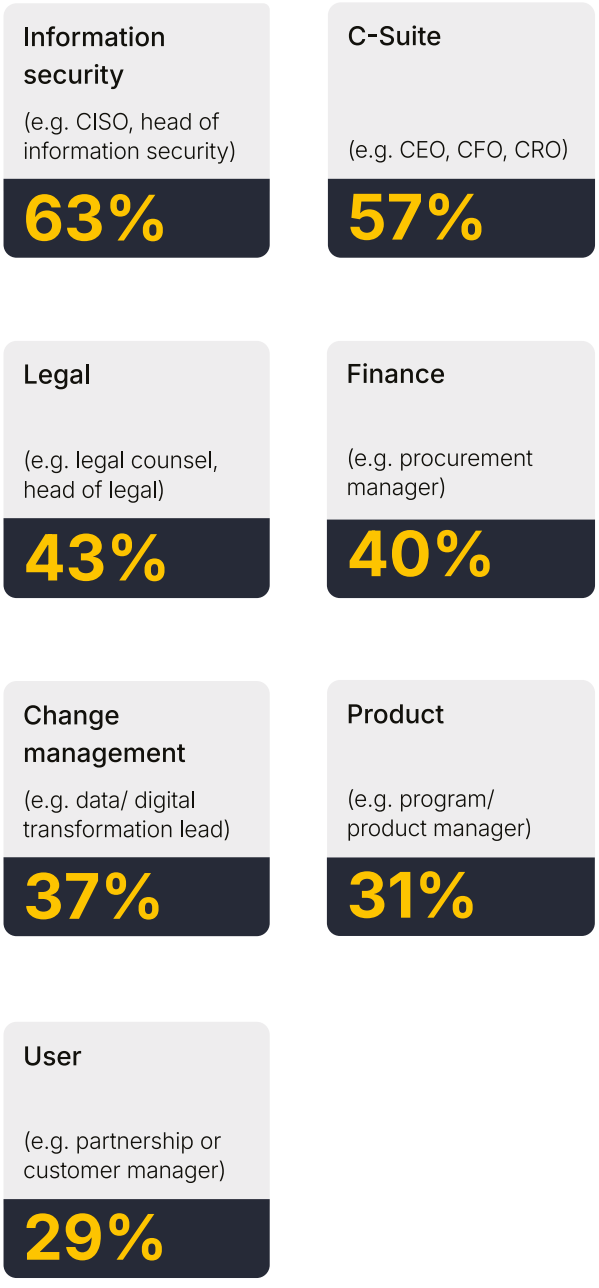
The survey also found this was not always as easy as it sounded. Our respondents noted ongoing challenges with getting key internal stakeholders on-side when upgrading systems or implementing new solutions. While some reasons for these problems were unsurprising – the cost of systems, perceived regulatory attitudes, legal and procurement requirements, and internal politics are well-known barriers – others, especially technology-specific concerns, appear to have become increasingly important. Indeed, the top two barriers selected by respondents were technological compatibility (53 percent) and Information Security (InfoSec) policy (48 percent), with the more traditional problems of cost and budget coming in third (at 43 percent).

What are the main barriers, if any, to implementing a new or upgraded solution in the compliance function?



Compliance leaders further noted the concern with getting InfoSec right when selecting the most important internal stakeholders to engage in upgrading technologies. Our survey found that respondents judged InfoSec to be the most important (63 percent), followed by the C-suite (57 percent), legal (43 percent), and financial team (40 percent).

When seeking to make substantial changes to your firm's compliance tech stack, which stakeholder groups do you need to consult?



Source: ComplyAdvantage, The State of Financial Crime 2025

What does this mean for me?

- Pay close attention to the fluid economic, regulatory, and risk environment that will persist through 2025 and beyond. There is little stability in any of these spheres, and developments in any of the three could combine to amplify negative effects.
- Look for compliance tools that are agile and flexible in this varied environment. These tools should provide robust risk data with the potential for wide functionality and integration.
- Consider carefully selecting vendors and partners, especially regarding high-priority criteria such as effective information security. Engage vendors and internal stakeholders early on these questions (e.g., during the RFP) to ensure your internal requirements can be met before too much time is invested in testing a platform your organization won't support.

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

Spotlight on organized crime

As noted, organized crime (see box) plays an increasingly dominant role in global criminality, enabled by the globalization of trade and travel, the rise of the internet, and communications technology such as smartphones. In December 2023, the UN Security Council (UNSC) – divided on so many other issues – held a debate on the scale and scope of organized crime, which emphasized the need for states to develop a better intelligence picture of criminal markets and their intersection with conflict zones, and to share best practice on policy and responses.

In 2024, the growing role of organized crime in economic and financial crime has been clear despite the setbacks to the broader globalization trends. OCGs have continued to make the most of the vulnerabilities they can find, especially through the abuse of new technologies. They have, moreover, shown themselves adept at finding new markets into which they can expand and diversify. The following section highlights several key developments in the core areas of OCG activity, as well as several expanding areas that are likely to continue to grow into 2025 and beyond.

What is organized crime?

The UN Office on Drugs and Crime (UNODC) defines organized crime as a "continuing criminal enterprise" that seeks "to profit from illicit activities that are often in great public demand." Organized crime is typically conducted by groups of varying sizes operating within and across geographies, commonly known as organized crime groups (OCGs). OCGs do not necessarily specialize in particular crimes, with their operational choices driven by the potential for making large profits with low risks. This said, most OCGs have at least some involvement in one or more of organized crime's 'core businesses': the illegal traffic of drugs, people, animals, and weapons.

Core business: The global drug market

2024 has seen several major law enforcement successes against OCGs involved in the illegal narcotics trade. Authorities on just about every continent recorded massive busts of narcotics in production or transit throughout the year. In January, Ecuadorian law enforcement seized around 22 tons of cocaine worth around $1.1 billion, hidden on a farm. In February, UK law enforcement seized 5.7 tonnes of cocaine from a container at Southampton's port, worth an estimated value of over £450 million.

In the spring of 2024, agencies from 31 countries, coordinated by the international police agency INTERPOL, seized over 615 tonnes of illicit drugs and precursor chemicals worth $1.6 billion.

Alongside these seizures, authorities also caused several operational disruptions for major OCGs. In July, US law enforcement officers arrested Ismael Zambada García, also known as 'El Mayo,' and Joaquín Guzmán López, both major figures in Mexico's Sinaloa cartel.

Following the arrests, infighting between the cartel's factions was reported to have escalated, with some cartel members believing that Zambada had been betrayed to the US authorities by López, whose own arrest was alleged to have been purely for 'cover.'

However, despite these successes, the scale and range of the global drugs market remained vast, shocking, and arguably one of the most resilient aspects of the global shadow economy. In June 2024, UNODC issued its annual World Drug Report 2024, which noted both a "record demand and supply" of well-known narcotics, as well as the growing use of new synthetic opioids. According to the report, the number of people using illegal drugs globally in 2022 was 292 million by 2022 – a 20 percent increase from 2012. Cannabis, opioids, amphetamines, cocaine, and ecstasy were the most used drugs in that order. UNODC particularly highlighted:

- **A "surge" in the cocaine market**, with increasing violence throughout major supply routes from Latin America, the Caribbean, and into Europe.
- **The rise of nitazenes** – synthetic opioids more addictive than fentanyl – began to account for a growing number of deaths by overdose in the developed world.
- **The impact of decriminalizing cannabis** and/or the legalization of its production and sale for non-medical uses in many jurisdictions has led many OCGs to diversify into higher-strength cannabis products.
- **The "psychedelic renaissance"** in the developed world led to a growth in the market for the illegal and unsupervised use of psychedelic drugs such as psilocybin and LSD.

The UNODC's one guarded cause for optimism was a decline in the market for opium and its derivatives, chiefly heroin, with global production falling by 73 percent in 2023, hit chiefly by the Taliban's decision to quash the drug's production in Afghanistan after its return to power in 2021. However, the agency also stressed that substantial amounts of opium remained on the market, supported by existing OCG stockpiles and rising production in Myanmar.

Emerging drugs trends

Within the overall landscape of illegal narcotics trafficking, 2024 has witnessed multiple examples of OCGs finding ways to maintain profits and innovate around problems. Following increasing attempts by North American authorities to prevent the supply of Asian-origin precursor chemicals needed for the production of synthetic drugs, Mexican law enforcement found local cartels producing their own rather than importing them from China. Latin American groups also found ways to evade interdiction at ports, with the growing use of unmanned self-propelled semi-submersibles (SPSS) to transport drugs at scale. The cartels have also sought to open new markets for synthetic opioids and methamphetamine beyond North America, including smaller European jurisdictions such as Ireland.

A further concerning development has been a growing confluence between the drugs-related activities of OCGs, terrorist groups, and several rogue states. There have been ongoing allegations in recent years that the Venezuelan government, drug cartels, factions of the revolutionary left-wing guerrilla group FARC, and Lebanese Hezbollah have conspired to generate funds from narcotics smuggling. More recently, there have been growing indications of a tightening relationship between the regime of President Assad in Syria, Hezbollah, and OCGs in the global supply of the amphetamine-like drug Captagon, the surge in demand for which in the states of the Persian Gulf has proved a major source of income for Assad. The growth in the Captagon trade, flowing across Syria's borders towards the Gulf through smuggling routes in Jordan, Iraq, and Saudi Arabia, has also led to major international frictions, even including armed clashes between smugglers and Jordanian security forces on the Syrian-Jordanian border.

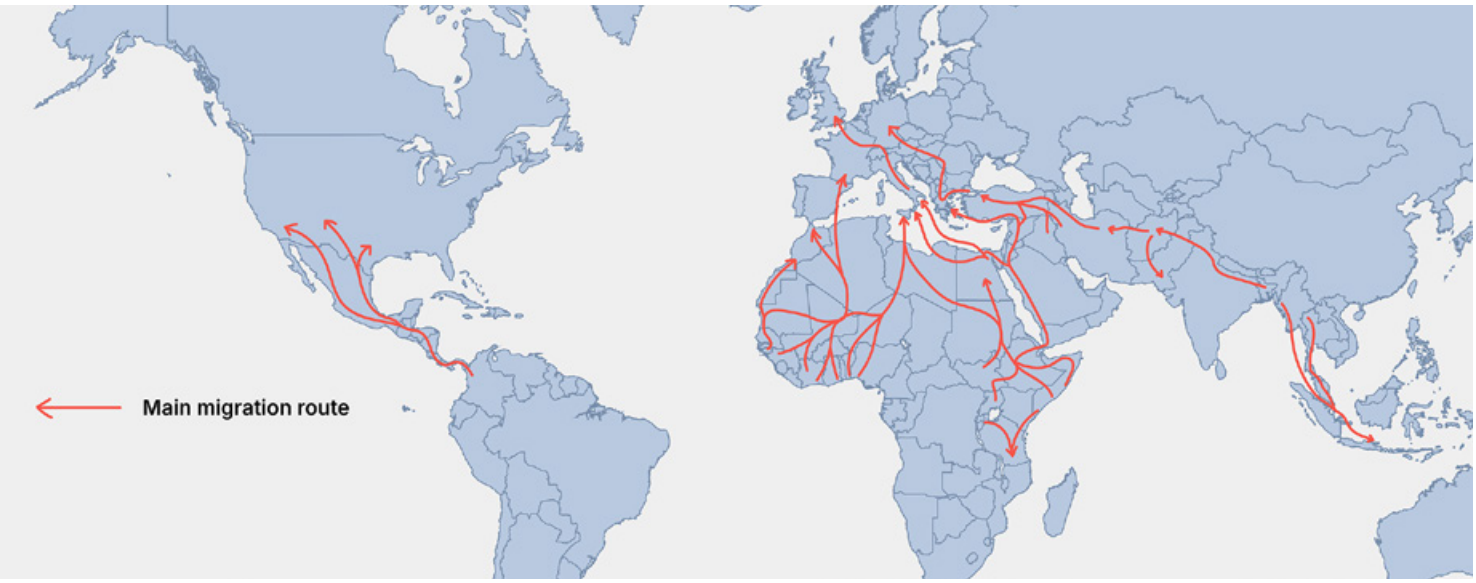
Core business: Human trafficking

Another core pillar of organized crime is the illegal movement of people within countries and across borders. The criminal movement of people is usually divided into two categories – human trafficking and illegal migration – although often there are substantial overlaps. In human trafficking, people are transported against their will and are usually exploited for various forms of illegal labor or sex work. This is often referred to as 'modern slavery.' In illegal migration, individuals seeking to migrate pay smugglers to transport them into countries they would not otherwise be legally able to enter. However, illegal migrants themselves can often be vulnerable to exploitation by OCGs, and illegal migration can often turn into human trafficking when smuggling OCGs decide to take advantage of their customers.

Violent coercion remains one important way for OCGs to source individuals for criminal exploitation. However, their techniques have become more subtle, too. One increasingly popular technique for recruiting sex workers is to use 'visa brokers' to attract women with the offer of jobs or educational development. In a similar vein, one of the major growth areas in human trafficking is known as 'forced scamming,' when individuals are typically lured into scam centers in remote locations overseas, where they are required, under threat of violence, to work for OCGs as online and phone-based scammers. These individuals are often unwittingly recruited through online job adverts that promise well-paid IT or financial services roles. When offered the job, they travel to the overseas destination, are met at the airport, and then have their passports confiscated before being taken to the scam center.

Illegal migration also remains a persistent area of OCG activity, with major routes flowing from South through Central to North America, from Africa and the Middle East into Europe (and within Europe to northern jurisdictions such as the UK), and from Southeast Asia into Oceania (see map below). Many of these routes have become increasingly 'industrialized' over recent years. Ad hoc or disorganized smuggling networks have become better coordinated and have attracted the involvement of existing OCGs looking for new opportunities to profit.

Some of the most significant flows, especially those from Africa and the Middle East, are driven by economic hardship, political instability, and war. Indeed, widening conflicts in Europe, the Sahel, and the Middle East have played a major part in the recent evolution of both human trafficking and illegal migration. The conflict in Ukraine, for example, has provided opportunities for human trafficking rings to source displaced Ukrainian children and women for sexual exploitation, as well as to traffic foreign men to fight on the Russian side, as in an instance identified by the Cuban government in September 2023. The Gaza conflict, too, has played into the hands of OCGs, with Palestinians seeking to escape the area paying brokers up to $10,000 to help smuggle them into Egypt, according to an investigation by UK newspaper The Guardian.



Source: IOM, UN Migration

Core business: Environmental crime

In the last two decades, environmental crimes – including illegal wildlife trafficking and the illicit exploitation of natural resources – have become, according to INTERPOL, one of the four main areas of global organized crime. Europol, the EU police agency, estimates that the annual value of transnational environmental crime is between $70 and $213 billion annually. Major elements of this criminal sector, of which numerous cases have been reported in 2024, include the trade in live animals as pets, animal parts used as food – often called 'bushmeat'– or as ingredients for traditional medicines in Asia, and the supply of endangered plants and timber, especially rosewood, from West Africa.

One of the notable trends in 2024, however, has been OCGs' increasing involvement in illegal mining in South America, where it has gained the nickname 'the new cocaine.'

Although various metals and minerals are mined, the primary target has been gold, following the massive rise in global prices over the last twenty years. In Ecuador, for example, the Los Lobos group has increased its involvement in illegal gold mining in nearly a third of the country's 24 provinces and has moved to control many parts of the supply chain. Such ventures are, of course, illicit in themselves. Still, they often prove to have an additional 'ripple effect,' bringing other crimes in their wake, including environmental damage and the exploitation of residents. In Peru, illegal gold dredging amongst the indigenous Awajún communities living along the Marañon River has brought with it petty crime, violence, and the sexual exploitation of local women and children.

OCGs have also shown signs of expanding operations in previously niche markets or opening up new sectors of environmental crime. The global rise in avocado consumption since the mid-2010s has led Mexican cartels to establish illegal avocado orchards to meet the rise in global demand. Mexican authorities estimate that 80 percent of the avocado orchards in the Mexican state of Michoacán, home to the Michoacán Family cartel, have been established illicitly, often using unauthorized land and the support and protection of corrupt officials. As with illegal mining, this criminal involvement in farming has led to a rise in environmental damage, exploitation of local people, and violence against civilians.

Core business: Trafficking weapons

The use of violence by organized criminal groups highlights a further area of persistent OCG activity – the trade in illegal weapons, especially small arms and light weapons (SALW). In 2024, the major arms markets have been centered in well-known zones of instability, such as:

- Latin America, driven by cartel activity and terrorist insurgencies, such as FARC;
- The African Sahel, driven by civil war, terrorist insurgencies, criminal gangs, and outside intervention by private military contractors such as Russia's Wagner Group, and;
- The Greater Middle East is fostered by the activities of territorial terrorist groups and militias such as Hezbollah, Hamas, and the Houthis, and criminal gangs and smugglers.

Conflict and the illegal arms trade are intimately linked, both creating a demand and a supply. Indeed, illegal weapons are most often sourced by theft from law enforcement agencies and military arms depots or by interception during transport. However, although more peaceful and stable locations – western Europe, for example – are relatively less affected, instability in surrounding areas such as the Balkans has stimulated the growth of the illegal arms trade and provided OCGs with opportunities to source and sell weaponry.

Unsurprisingly, therefore, one of the biggest growth areas in recent years for illegal weaponry has been the conflict in Ukraine, and research suggests that the country has become a pool of illegally diverted arms. A US Defense Department report from early 2024 indicated, for instance, that around 60 percent of the weapons the US had supplied to Ukraine had gone "delinquent" from controlled stockpiles and were no longer tracked on databases. Many of these weapons are likely to have moved into the hands of criminals. Indeed, as the Global Initiative Against Transnational Organized Crime (GI-TOC) has noted this year, there are growing indications that what started as a large and fluid arms market in Ukraine has become much better organized, suggesting the growing role of OCGs. Of even greater concern, however, is the sophistication of the weapons involved, including kamikaze and switchblade drones, anti-tank missiles, and shoulder-fired missiles. Even if the war in Ukraine were to cease in 2025, the role it has played in bringing such advanced weaponry onto illicit markets will be felt for many years to come.

Core business: Counterfeiting

INTERPOL notes that other core elements of the organized crime trade include armed robbery, money laundering, and counterfeiting. Armed robbery is largely a domestic rather than transnational phenomenon, so it is not our focus in this report. Money laundering is another matter, however – a major global problem, both as an aspect of organized criminality and as a professionalized criminal industry in its own right. This leaves counterfeiting of high-value or hard-to-access goods, such as jewelry, designer clothes, luxury cars, and major international currencies, such as the US dollar and the Euro.

E-commerce has been a major enabler of the trade in counterfeit goods, especially facsimile pharmaceuticals.

In September 2024, a US advocacy group, the International Coalition Against Illicit Economies (ICAIE), reported that $4.5 trillion of the $20 trillion generated by global e-commerce in 2023 had been in counterfeit goods. During the year, Europol and other agencies also warned of the growing online trade in counterfeit medicines, especially for performance enhancement in sports, painkillers, sexual aids, and so-called 'nootropics,' which allegedly boost cognitive performance. A further growing concern has been the online trade in illegal car parts, highlighted by the European Union Intellectual Property Office (EUIPO) in 2024. According to the agency, most of these parts have come onto the market from China and Hong Kong, accounting for 60 percent of global seizures of dangerous products destined for the European market. Quite apart from being an infringement on intellectual property (IP) rights, such parts are also dangerous, often falling short of international safety standards and putting car drivers at serious risk.

Growth areas: Illegal gambling

As suggested by their expansion into new areas of environmental crime, OCGs have also been expanding in other areas beyond their core businesses. One notable sector of growth has been illegal gambling and the manipulation of sporting events. The UN anti-corruption conference in Atlanta at the close of 2023 highlighted the rise of illegal betting and the role OCGs and transnational syndicates played in its rise. According to UNODC figures from 2021, up to $1.7 trillion is bet annually in illegal markets managed by organized crime, and OCGs play a primary role in the fixing of professional matches in major international sports such as soccer. Several specific examples of OCG activity in sports and betting came to light in 2024 in Asia and Europe, especially around major sporting events. An operation involving INTERPOL and 28 countries and jurisdictions, code-named SOGA X, led to over 5,100 arrests and the recovery of more than $59 million of illegal bets on the Euro Soccer Championships in the summer of 2024. However, soccer was not the only targeted sport. In the spring of 2024, Spanish authorities announced the disruption of a network linked to fixing soccer, tennis, and table tennis matches in more than 20 countries, which accrued illicit proceeds estimated to be around €2 million ($2.2 million). The same network was also involved in illegally selling personal data from betting platforms.

Core business: Extortion & racketeering

A further growth area for organized crime has been extortion and protection racketeering, where criminals threaten violence against their target if they do not meet a demand or pay for an unwanted product or service. In the last year, this trend has been most obvious in Latin America:

- In Ecuador, authorities estimated that extortion cases had risen by almost 400 percent since 2021, with common types of extortion involving threatening phone calls (most often coming from prisons), demands for periodic payments to protect individuals and businesses, and sexual blackmail.
- In Colombia, reports of extortion to the police rose massively; in the Atlántico department, case numbers rose from 199 in 2019 to 1,335 in 2023 – a 570 percent rise.
- In Venezuela, OCGs moved from extorting traders, cattle ranchers, and fishermen to local residents and schools.
- In Mexico, cartels extended both the sources of extortion and their range of targets. In Michoacán, one cartel created its local Wi-Fi network using unofficial internet antennas. It coerced local residents into paying above-market rates, generating about $150,000 a month for the group.

This growing attraction to extortion appears to have been largely driven by Latin American OCGs' need to diversify their income sources because of the highly competitive character of the region's drug trade. However, extortion is not just a Latin American phenomenon. In the spring of 2024, Europol noted its use by several of the most dangerous criminal networks operating in southern European jurisdictions such as Greece.

The impact of organized crime

Regulated firms can often lose sight of the central role that organized criminal groups play in the economic and financial crimes that their compliance controls are meant to prevent, detect, and mitigate. There is a persistent danger that firms will become more obsessed with the minutiae of AML/CFT policies, procedures, and controls than with the overarching problems that necessitate them in the first place.

It is important to remember the wider impact of organized crime. It is undeniably staggering, even in the abstract. UNODC notes that in 2009, it was estimated that transnational organized crime was generating $870 billion, around 1.5 percent of global GDP. That absolute figure of illicit income generated by organized crime is likely to be much greater now, especially as OCGs expand, innovate, and diversify. Economically, this translates into lost tax revenues, lost jobs, and market distortions. The EUIPO has estimated that counterfeit goods cost the European clothing, cosmetics, and toy industries €16 billion (around $17.5 billion) in sales and 200,000 jobs a year. However, the impact goes far beyond headline figures to directly affect individuals, families, communities, and the environment. The sale of illicit items trafficked by OCGs – drugs, counterfeit items, for example – will potentially harm someone – whether it is the buyers or those around them.

The growing sale of illegal weaponry supports higher rates of violence, while human trafficking and illegal migration trade on and magnify human misery, often amongst the most vulnerable people. Impacts should never be underestimated, moreover. The growth in illegal but supposedly low-risk cannabis derivatives in North America has led, for example, to a rise in psychiatric disorders and attempted suicide amongst users, especially the young. At the same time, environmental crimes lead to pollution, deforestation, the degradation of land and water, the reduction of biodiversity, the extinction of rare wildlife, and the erosion of indigenous communities.

All told, organized crime has been a force multiplier for the very worst aspects of human behavior.

Organized crime in 2025

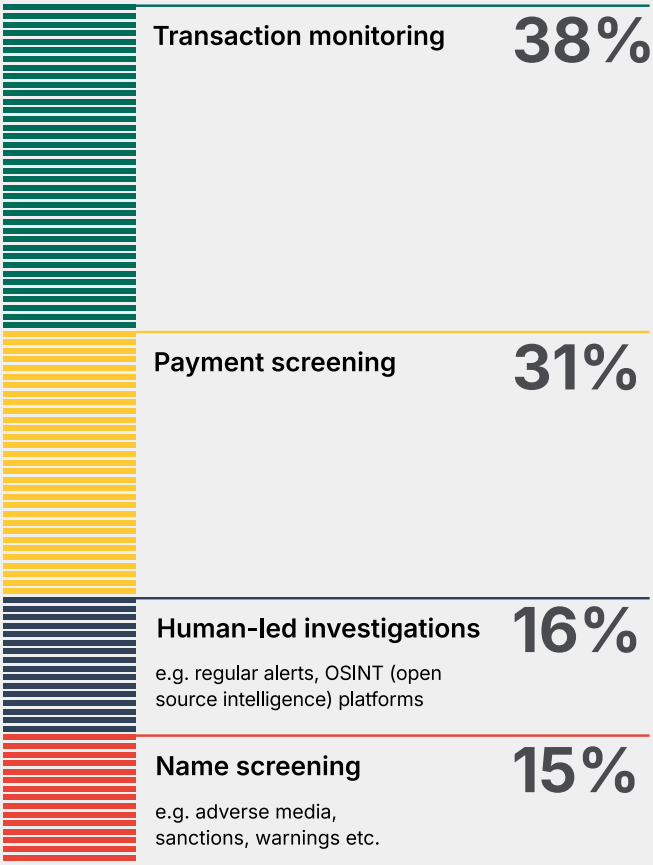
Over the last three decades, organized gangs have integrated themselves into the global economy, catering to illegal demand and generating profits from the sufferings of others. Based on the findings and investigations of researchers and law enforcement agencies, OCGs have largely succeeded and, as the evidence from 2024 indicates, have continually found new ways of doing so. Organized crime keeps evolving, seeking new methods, opportunities, and vulnerabilities. This suggests that 2025 will be another year where, despite some law enforcement successes, OCGs will prove their resilience. One trend you should pay particular attention to is the increasing role of organized crime in legitimate markets, where massive rises in global demand have led to shortfalls of licit supplies; the case of gold mining and avocado cultivation, for example, are important harbingers of potential future developments.

Compliance leaders' perspectives on organized crime

Our survey suggests that businesses are extremely aware of the risks of exposure to organized crime, with 71 percent of organizations saying they already undertake a detailed analysis of exposure to organized crime in their financial crime risk assessments and a further 26 percent saying they plan to undertake one in the next 12 months.

How firms detect real-time exposure appears to rely on diverse methods, with 39 percent of respondents emphasizing transaction monitoring, 31 percent payment screening, 16 percent human-led investigations, and 15 percent name screening. This suggests that firms do not see any one platform as sufficient on its own and are using multi-pronged approaches as they seek to identify and mitigate the risks.

Which source does your organization primarily use to identify potential organized crime?



Source: ComplyAdvantage, The State of Financial Crime 2025

What does this mean for me?

- Organized crime is undoubtedly the major global driver of economic and financial crimes. Tackling it should be the fundamental goal not just of law enforcement agencies but also of businesses potentially exposed to its activities, especially the regulated financial sector.
- Your team's approach should go beyond tick-box compliance to thinking in detail about your company's potential exposure to particular types of crime and crime typologies. Policies, procedures, and controls need to be agile, flexible, and open to recalibration.
- Technology will play a major role in helping generate insights about potential OCG exposure, especially by leveraging integrated platforms and comprehensive risk data sets.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

Wider crime trends

Separating out predicate crimes committed largely by OCGs from wider crime trends is in some ways misleading, as OCGs themselves are involved in various degrees to other types of crime beyond their 'core trades.' However, in a range of other major areas of criminality, OCGs sit alongside a spectrum of other criminal actors of varying scale and levels of organization. While some OCGs are certainly heavily involved in cybercrime, fraud, bribery, and corruption, they are not exclusive provinces of organized crime, at least at present. The following sections, therefore, look at these other areas of major criminality that have particular significance for the regulated sector.

Cybercrime

Cybercrime largely falls into two broad areas – the exploitation of the surface and dark web for the sale of illicit goods and the use of cyber hacking to steal, extort, and ransom funds from businesses, organizations, and individuals. Although the law enforcement agencies of the US and other states have undertaken sustained disruptive action against major dark web marketplaces such as DarkMarket, Hydra Market, and Genesis, illicit online markets have still continued to grow, providing a range of products and services from the sale of well-known illicit items to ID documents, credit card details and other criminal paraphernalia.

One of the most troubling developments in dark web activity in recent years has been the growth in the sale of illegal sexual material, described as child sexual abuse material (CSAM) or online child sexual exploitation (OCSE). According to an investigation reported in early 2024 by the Internet Watch Foundation (IWF), an advocacy group, more than 275,000 web pages reviewed contained CSAM, an 8 percent increase from the previous year. Research by blockchain risk consultancy Chainalysis, as well as reporting from the US Treasury's Financial Crimes Enforcement Network (FinCEN), suggested that a substantial amount of the trade-in CSAM was being transacted in cryptocurrencies and that vendors were increasingly turning to privacy coins to reduce official surveillance. Nonetheless, other payment methods, including peer-to-peer payments in fiat currencies, often on the open internet, also continued to play a role.

An investigation by The Guardian, reported in March 2024, alleged that CSAM was being traded via a major social media platform, with its peer-to-peer payment service being used to pay for the items.

Beyond illicit online markets, the internet also continued to be an attractive avenue for other forms of cybercrime.

Law enforcement authorities had some successes against hackers in 2024. In February, INTERPOL revealed the outcome of Operation Synergia, which identified 1,300 suspicious IP addresses and URLs used for phishing, malware, and ransomware attacks. Also in February, Europol reported an international operation across Europe, the US, and Asia Pacific to take down the critical infrastructure behind LockBit, one of the most widely used 'ransomware-as-a-service' tools, offered by a team of cyber criminals that license out malware code.

Despite these law enforcement successes, cybercriminals have become increasingly professionalized and adept. According to Chainalysis, 2024 is likely to be the highest-grossing year on record for crypto ransoms. July 2024 witnessed a crypto ransom payment worth $75 million to a group known as Dark Angels, the biggest ransomware payment ever recorded. Crypto hacking has also been on the rise after a major drop in 2023. While Chainalysis found a comparable number of hacking incidents between the mid-years of 2023 and 2024, it also found a massive rise in value extracted in 2024 – around 79.5 percent – partly reflecting the rising exchange value of cryptocurrencies such as Bitcoin.

A significant proportion of these hacks were focused on centralized cryptocurrency exchanges (CEX) after several years where decentralized exchanges had been the main target. A major example of the re-targeting of CEXs was the hack of the Japanese DMM exchange in May 2024, which lost the equivalent of $305 million in bitcoin.

Cybercriminals also expanded their use of certain exploitative methods in 2024. 'Sextortion,' a technique in which cyber criminals target young people via social media, encourage them to send them sexually explicit material, then threaten to distribute the images unless payment is made, is on the rise, especially in the Anglophone world. In the UK, the IWF found a 19 percent increase in reported sextortion cases in the first half of 2024, a similar pattern to that seen in the US and Australia. A report published in January 2024 by the US advocacy group the Network Contagion Research Institute (NCRI) indicated that much of the activity was emanating from cyber criminals based in West Africa, known as 'Yahoo Boys,' who targeted individuals in the developed world and were often lauded in local popular culture as heroes.

Cybercrime in 2025

Despite rising public awareness and law enforcement successes, cybercriminals have continued to use the internet to sell illicit goods and services successfully. In many ways, law enforcement is playing 'whack-a-mole' with cyber criminality; when one marketplace is taken down, others take up the slack in the online market for illicit goods, or new ones rise in their stead. As long as the dark web exists, access to it is legal in many jurisdictions, and human desires for illicit goods persist, it is liable to provide an enduring enabling environment for criminal activity. In parallel, the use of the internet as an avenue for theft and ransoms will also continue, especially given the relatively low levels of cyber security and cyber hygiene in many businesses and organizations. While many hacks are dependent on previously unknown vulnerabilities, so-called 'zero-day exploits,' many still take advantage of easily foreseeable gaps in system protections and human fallibilities. There is little sign of that changing in the near future.

Financial fraud & scams

Alongside cybercrime, financial fraud – achieving financial gain through deception – is another major area of criminal activity involving organized rings, smaller and more disorganized criminal groupings, and individual fraudsters. According to the INTERPOL Global Financial Fraud Assessment, published in March 2024, financial fraud is "increasingly dependent on information and communication technologies," making "fraud operations ... transnational and often transcontinental" and "a pervasive, global threat."

National figures suggest that in some countries, the problem has become endemic; figures from the UK Financial Ombudsman, released in September 2024, indicated that the UK had suffered more than 8,700 fraud and scam cases between April and June of that year, a 43 percent increase in the figures from the same period in 2023, and the highest level ever recorded in the UK. As INTERPOL and other law enforcement agencies have noted, those targeted by fraudsters are typically vulnerable individuals at the extreme ends of the age scale. In its annual data book, released in February 2024, the US Federal Trade Commission (FTC) noted that both the young and the old were the main targets of fraudsters, with the youngest adults most defrauded by a number of cases, and older adults defrauded by the highest amounts.

Imposter frauds

The most prevalent types of contemporary fraud are impostor scams – where the fraudster(s) pretend to be a trustworthy figure, whether that be a figure in official authority, a bank's fraud team, a familiar business, or a relative or friend. They then use this supposed credibility to take funds, assets, or personal data under false pretenses. In the US, the FTC assesses that

impostor scams are the largest class of frauds by loss volume, with its annual data book reporting losses of $2.7 billion in 2023.

The most common type of impostor scam in many countries is authorized push payment (APP) fraud, where the victim makes the 'authorized push' of the payment from their own account to one controlled by the fraudster. APP has many versions, including 'malicious payee' ploys or 'purchase scams,' where the fraudster creates a business front that 'sells' a fake product or service to an unsuspecting victim, who then makes a payment but receives nothing in return. Much of this type of fraud now takes place online via e-commerce, as an investigation by several major newspapers – The Guardian, Die Zeit, and Le Monde – published in May 2024 showed. In an investigation of what is believed to be one of the largest frauds of its type, journalists identified 76,000 fake online designer shops operated out of China, which had already duped more than 800,000 victims in people in Europe and the US, selling fake items and stealing financial and personal data.

A further variety of APP is known as 'malicious redirection,' where a fraudster posing as an authority figure asks the victim to transfer funds to a different bank account controlled by the fraudsters or into an alternative receptacle of value, such as cryptocurrency or even a gift card. Another common impostor-style fraud that uses fake authority figures to redirect bank account payments is one that typically affects businesses rather than individuals. It combines common cyber hacking and impostor techniques. In Business Email Compromise (BEC), the emails of senior figures within a business, or potentially those of a major supplier to the company, are 'spoofed' and then used to send messages to members of staff at the targeted firm, requesting them to make payments to what appears to be a legitimate account, but one in fact controlled by the fraudsters.

However, bank account transfers are not the only means fraudsters use. In the UK, for example, courier fraud has become a massive problem, especially for seniors. In this style of fraud, victims are contacted by individuals who claim to be from the police or a bank and who tell them their accounts have been compromised by fraudsters. They then warn them that they need to transfer their money and assets to a safe location and offer to help. One of the fraudsters will then turn up at the home of the victim, posing as a police officer, a member of bank staff, or even a courier, to collect items such as debit and credit cards, PIN numbers, valuables, and money, to take them for 'safekeeping.' According to figures reported in May 2024 by the City of London Police, British pensioners lost £28.7 million to this type of fraud in 2023, with an average loss per victim of £20,000, and some individual cases where victims lost as much as £5.3 million and £1.9 million each.

Investment and founder frauds

Investment scams, where fraudsters convince unsuspecting investors to put money into supposedly new or growing products or companies or supposedly under-valued stocks, have been another major category of fraud in 2024. Early in 2024, court cases in the US highlighted classic examples; in one, an individual was charged for falsely claiming to run a cash-rich corporate group of cellular and agricultural companies in Nigeria, and in another, example the fraudster used investors' interest in emerging technology to gather funds for non-existent start-up manufacturing and converting electric vehicles (EVs) and natural gas-powered cars.

Cryptocurrency ventures have also proved to be a particularly fruitful area for fraudsters. In March 2024, Sam Bankman-Fried was sentenced today to 25 years in prison and ordered to pay $11 billion as a consequence of several frauds conducted through FTX, one of the world's largest CEXs, and the cryptocurrency trading firm Alameda Research, both of which Bankman-Fried founded. However, he was far from being a one-off in the sector. In January 2024, the US Securities and Exchange Commission (SEC) charged Australian entrepreneur Sam Lee with fraud for his involvement in HyperFund (also known as 'HyperVerse'). This alleged crypto-asset pyramid scheme took more than $1.7 billion from investors worldwide. In May, three executives of the bankrupt crypto-lending business Cred were also charged with fraud in California or causing losses exceeding $780 million in value with a scheme that falsely promised collateralized and guaranteed lending. And in July, self-exiled Chinese national media mogul Guo Wengui was convicted in New York of a $1 billion fraud, where investors were encouraged to put money into a crypto-asset referred to as 'Himalaya Coin' or 'H-Coin,' which he claimed to partially back by gold.

Western countries have not been the only jurisdictions to witness massive frauds by major business leaders, however.

Most notably, in April 2024, Vietnamese billionaire and property mogul Truong My Lan was sentenced to death after being convicted of orchestrating a fraud worth $27 billion. According to the prosecution case, $12.5bn was embezzled from the company, equivalent to around 3 percent of the Vietnamese GDP. Ms Lan was also aided by over 80 associates, all of whom were found guilty but faced lesser sentences.

Romance + investment = pig butchering

Romance fraud has been another growing phenomenon in the last decade, tracking the rise of social media and online dating, with fraudsters posing as potential partners who request financial 'help' from their targets. According to UK Finance, a business association representing the UK financial services industry, it has become a massive challenge for the sector, with the number of reports of such scams rising by 58 percent in the UK between 2019 and 2023. Increasingly, romance scams have also made use of GenAI to create fake images, videos, and voice recordings of supposed 'love interests' being used as cover by fraudsters.

A further trend in 2024 has been the growth of a scam known as 'pig butchering,' which combines elements of romance and investment fraud. In pig butchering schemes, fraudsters initiate relationships with victims through social media, dating sites, and even random text messages. Eventually, they encourage the victim to invest in fraudulent cryptocurrency investments, after which they disappear, taking the money with them. As INTERPOL has reported, many pig butchering schemes are run through the previously mentioned 'scam centers' in Southeast Asia, West, East, and Southern Africa, Eastern Europe, and Latin America and are staffed by victims of human trafficking. According to the agency's 2024 Global Financial Fraud Assessment, this fraud technique is "escalating and expanding" and is probably underreported, with many victims too embarrassed to report the crime.

Fraud in 2025

Fraud will undoubtedly continue to be a major source of illicit revenue in 2025, with criminals leveraging the anonymity of the online world, basic human psychology, and relatively low levels of fraud awareness in vulnerable sectors of society to take advantage. The rise of pig butchering and courier fraud suggests that firms and their customers will face a more innovative and hybrid set of fraud methods in the coming years, as fraudsters 'mix and match' different types of fraud and use various communications channels to achieve an outcome. Advancing technology – especially GenAI tools that can create convincing representations of faces and voices – will also support and enable their activities. However, the rise of so-called AI-created 'deepfakes' should not blind businesses to the ongoing usage of tried-and-tested methods either. For fraudsters, what counts is what works.

Bribery & corruption

Two final predicate financial crime types worth highlighting for their significance in 2024 are bribery and corruption. Bribery commonly involves the demand for, or offer of, payments of cash or 'payments in kind' to secure favors. This is in itself a class of corruption, which can be more broadly defined as the misuse of positions of power, control, and access to extract personal gain or favors.

Kleptocracy

In recent years, western governments such as the US under President Biden have shown an increasing focus on official corruption in authoritarian or hybrid regimes, especially the misappropriation of public or assets by elite figures within or attached to regimes, often described as 'kleptocracy.' Following the full-scale invasion of Ukraine by Russia in February 2022, the kleptocratic behaviors of Russian oligarchs linked to the Putin regime re-doubled attention on this issue, and extensive financial sanctions have been imposed on those oligarchs closest to the Russian president – discussed in 'Geopolitics and Sanctions.'

Nonetheless, the kleptocratic problem is far from being resolved. In February 2024, the National Endowment for Democracy (NED), a semi-autonomous US Non-Governmental Organization (NGO), issued a report by journalist Ben Judah, suggesting that over $127 billion had been misappropriated and laundered by kleptocrats and their enablers around the world, including networks linked not only to Russia and the countries of the former Soviet Union, but many in Africa, South America, and Southeast and East Asia. According to the report, substantial amounts of illicit proceeds came from Foreign Direct Investment (FDI) into developing countries or humanitarian and development funds intended to support at-risk communities. In a recent case along these lines, Betta Edu, Nigeria's Minister of Humanitarian Affairs and Poverty Alleviation, was suspended in January 2024 and then removed from office in October – although not so far charged or prosecuted - after Nigerian naira worth $663,000 went missing from her department's funds. Edu has denied any wrongdoing.

Corporate bribery

A further strand of activity notable from media reporting in 2024 is corporate bribery involving Western multinational corporations and officials in emerging and developing markets. Cases against companies within major Swiss-based commodities groups featured prominently due to a major and ongoing investigation by the US Department of Justice (DoJ) into the bribery of state-owned hydrocarbon businesses in Latin America. In March, Trafigura pled guilty and agreed to pay over $126 million to close a US government investigation into bribes to secure business with Brazil's state-owned oil producer, Petrobras. Also in March, Gunvor S.A. pled guilty following a US investigation of a scheme involving the bribery of officials at the Ecuadorian Ministry of Hydrocarbons and Petroecuador, the country's state-owned oil company. In August, Glencore pled guilty to charges of bribery to advance its oil operations in Cameroon in a case brought by the UK Serious Fraud Office (SFO). Also in August, Javier Aguilar, a former trader for Swiss oil trader Vitol but based in Texas, pled guilty in the US to paying bribes in Mexico to officials at PEMEX Procurement International (PPI), an affiliate of the country's state-owned oil company, PEMEX. This followed his US conviction earlier in the year for bribing officials at Petroecuador.

However, other cases showed that bribery was not simply a problem for Swiss commodity firms operating overseas. In January 2024, SAP, a software company based in Germany, agreed to pay over $220 million in fines to resolve a DoJ investigation into the alleged bribery of government officials in South Africa and Indonesia. Media reports in June also indicated the existence of an internal investigation within German sportswear manufacturer Adidas into the payment of bribes in China, which led to the departure of two employees. And businesses from non-western countries also appeared willing to consider paying bribes. In September 2024, for example, South African police were reported to be investigating the operations of the Guptas, one of India's richest business families, around allegations of bribery related to contracts with the South African public electricity utility Eskom.

Political bribery

Of course, bribery does not only take place between businesses and governments in the developed world, and 2024 also highlighted a number of cases where Western politicians were alleged to have corrupt relations with foreign governments. Most spectacularly, New Jersey US senator Bob Menendez was found guilty in July of accepting bribes from two Middle Eastern governments in return for promoting their interests in Congress. The bribes included cash, gold bars, luxury cars, luxury watches, and sporting hospitality. There were also increasing concerns throughout the year in various Anglophone and European countries about the potential for Russian bribery of politicians and officials in order to promote its revisionist agenda. In March, for example, Czech authorities revealed a scheme, believed to be organized by Russian intelligence, to distribute funds to European politicians susceptible to Russian narratives via the Voice of Europe, a pro-Russian media platform. According to the Czech authorities, many hundreds of thousands of Euros were transferred to willing politicians via cash and cryptocurrency transfers.

Bribery & corruption in 2025

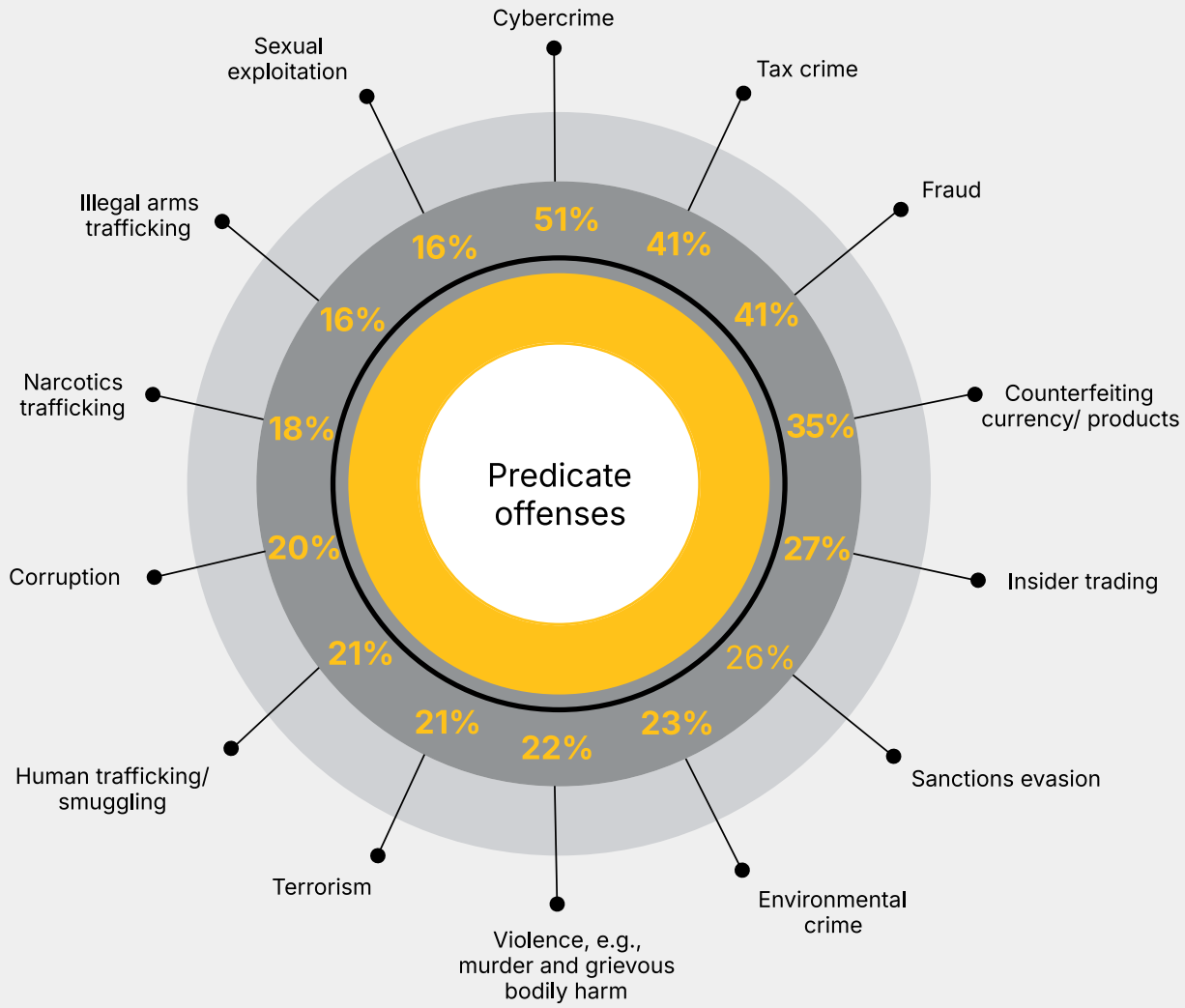
Bribery and corruption will remain a significant issue for many developed countries in 2025, although ongoing economic sluggishness in the most advanced economies might encourage some to turn a blind eye. Indeed, it is probable that Western governments will at least become more selective in the corruption they tolerate, with kleptocratic inflows from more friendly non-aligned states such as those of the Persian Gulf raising fewer concerns than those from more hostile competitors such as China and Russia. Inflows from these latter states will generate more political anxiety, interest, and political activity as they are increasingly tinged with concerns about espionage and malign influence. In addition, as the world becomes increasingly multipolar, we are likely to see increasing examples of large businesses from India, China, and other leading emerging markets appearing in cases of bribery in the less economically successful parts of the developing world. The Western world will not have a monopoly here any more than it does geopolitically or economically.

Compliance leaders' perspectives on cybercrime

Just over half of the respondents reported cybercrime to be the predicate crime on which they have expended the most time and resources in the last year, leaving it in the 'number one' spot that it also occupied in last year's survey. Tax crimes and fraud tied for second place at 41 percent each, followed by counterfeiting at 35 percent.

A mix of other concerns, such as insider trading, sanctions evasion, environmental crimes, violent crime, terrorism, human trafficking, and corruption, clustered between 20 and 27 percent. Interestingly, major crime types such as drug trafficking, illegal arms trafficking, and sexual exploitation came towards the bottom of the ranking, all falling below less than 20 percent.

Which of the predicate offenses below has your organization focused the most time and resources on over the last 12 months?



3% There are no predicate offenses my organization has focused time and resources on over the past 12 months

Source: ComplyAdvantage, The State of Financial Crime 2025

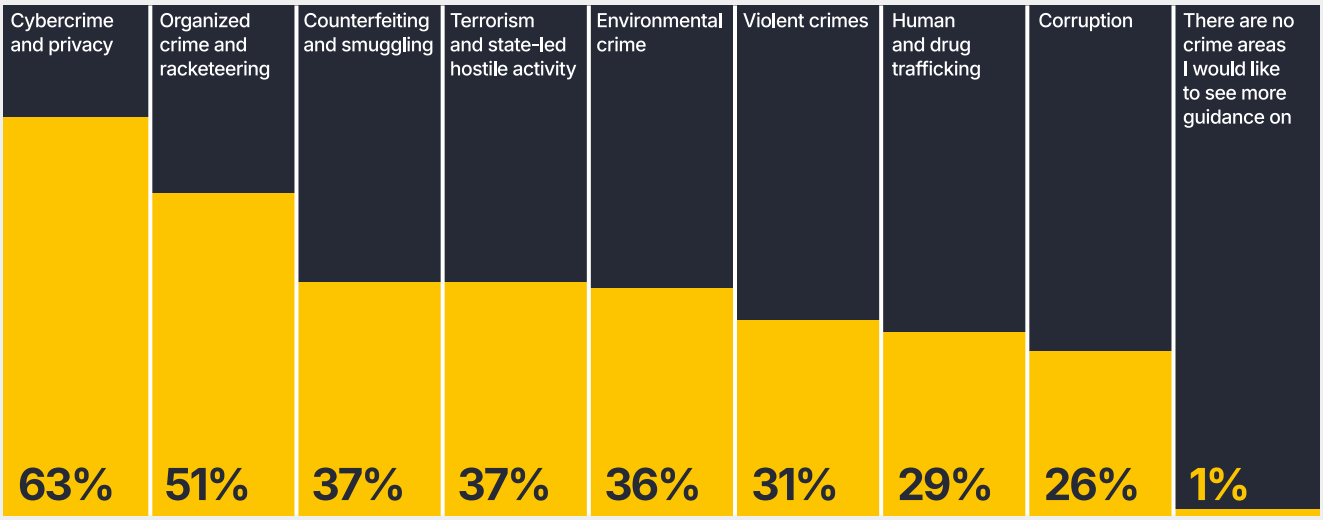
We also asked our respondents where they felt the most guidance was needed to tackle organized crime across a range of predicate offenses. Cybercrime and privacy led the way with a massive 63 percent – highlighting again the challenge cybersecurity is creating for the private sector. The second main area of concern was organized crime and racketeering, at 51 percent. In the middle, several clustered in the mid-thirties: Counterfeiting and smuggling (37 percent), terrorism and state-led hostile activity (37 percent), and environmental crime at 36 percent. The final three were violent crime (31 percent), human and drug trafficking (29 percent), and corruption (26 percent). In light of the heavy political, regulatory, and law enforcement focus on these last three areas in the past decade, it is perhaps not surprising that they are now lower priorities. What may be surprising is the relatively substantial score all three attained in those circumstances. The industry clearly still feels that authorities have a lot more that they can do to help it tackle crime.

What does this mean for me?

- The ongoing importance of cybercrime suggests that your team should look closely at its potential exposure to illicit online markets and the cybersecurity measures you have in place to protect your company and its customers. There is a justifiable concern that, in too many cases, firms are leaving their doors ajar for hackers.
- The scale, growth, and evolution of financial fraud remain a poisonous problem, especially if you work in a company exposed to e-commerce and with customer bases vulnerable to APP fraud. The best course of action is to advocate for investments in appropriate technologies that can adapt to detect and prevent new trends in fraudulent behavior at an early stage.
- Bribery and corruption also affect client relationships with many trading companies and important foreign and domestic officials. To understand where the greatest risks might lie, you need up-to-date and timely risk data – especially politically exposed person (PEP) lists and hard-to-find adverse media.

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

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 2025

Money laundering & terrorist financing

As we have highlighted in previous years, the infrastructure of the legitimate financial system – financial institutions, bank accounts, transfers, payments, etc. – remains absolutely vital to contemporary money laundering. The revelations of the last decade have shown the ongoing abuse of major Western banks by bad actors of all varieties, including organized crime, as well as financial institutions themselves struggling to deal adequately with the challenge, leading to recurring regulatory enforcement measures. And such cases are far from historic. In February 2024, for example, Europol reported the disruption of a Russian-Eurasian network operating out of Berlin and Latvia, which used a Maltese financial institution to launder at least 4.5 million Euros in illicit funds from 2015 onwards. The legitimate financial system clearly remains one of the major channels for moving illicit funds.

How money launderers achieve this is still, in some ways, surprisingly 'old school.' The use of legitimately cash-rich businesses in retail, hospitality, and entertainment continues to provide a relatively unimpeded avenue for OCGs to pay cash straight into the financial system. In the UK over recent years, critical observers have highlighted the growth of American-style themed candy stores on city and town high streets, with allegations that these shops operate as fronts for laundering and cover for other activities such as the distribution of counterfeit goods and narcotics. Similar accusations have been made about the proliferation of hand car washes and generic souvenir shops in major European countries, such as Amsterdam.

Another durable technique for getting dirty money into the system is the use of 'smurfs' – usually witting junior money launderers – to pay carefully structured funds into accounts at levels calibrated not to draw the attention of compliance teams, regulators, or law enforcement. The role of the smurf is also increasingly undertaken by money mules – individuals who are wittingly or unwittingly used to pay or receive illicit funds into their own accounts and then send those funds to other accounts.

Mules can operate in cash, but much of their work is now done electronically;

Europol found in 2016 that more than 90 percent of funds moved by mules actually came from cybercrime.

Many mules are also victims of crime themselves, having been trafficked for exploitation by OCGs. Others are vulnerable individuals – the unemployed young, students, the elderly, for instance – who get recruited through social media or face-to-face interaction with offers of an income from a simple activity, unaware that they will become accessories to criminal activity. The problem affects most countries across North America, Europe, and Asia-Pacific, with launderers increasingly seeking new locations and categories of potential mules to target. In early 2024, INTERPOL and the Irish police noted the growth of money mule activity amongst young people in Ireland, tracking the growth of the country's rise as an international financial center. In June, Australian authorities also noted how laundering networks were targeting international students and non-permanent residents for muling, both through social media and direct contact, usually offering them an easy way to make money during a temporary stay in Australia.

Moving money globally

Once illicit funds are in the financial system, launderers move them between various accounts, products, and channels before concentrating them in what appear to be legitimate business accounts and then transferring them to other business accounts overseas. These accounts are often held by shell companies that lack an obvious business purpose and can be located in major financial centers like the US, UK, Hong Kong, and Singapore, but also off-shore secrecy jurisdictions where the application of AML/CFT standards is perceived to be light.

Nonetheless, OCGs and money launderers are aware that washing large amounts of funds through the financial system will trigger concerns with financial institutions, and criminals have, therefore, become adept at transferring funds in other ways. The most important method for doing this remains trade-based money laundering (TBML). In TBML, criminals transfer value overseas by manipulating and misrepresenting the volume or value of goods being traded, ostensibly by legitimate companies, but in reality, within or between OCGs. Cargoes can be under or over-invoiced, and in some cases, 'phantom' cargoes can be used simply to create the justification for a cross-border transfer of funds, ostensibly for commercial purposes. Although no one knows the global scale of TBML, many experienced financial crime experts believe it is the most significant method for transferring illicit value overseas; in 2018, the International Chamber of Commerce (ICC), a global industry body, suggested that the value of TBML was likely to be in the hundreds of billions of US dollars. A further study issued in February 2023 by Global Financial Integrity (GFI), an advocacy group and think tank, estimated that around 80 percent of global illicit funds were moved via TBML, with mis-invoicing the most common technique and drug trafficking the most prevalent predicate offense.

However, international payments and TBML are not the only ways that funds are being transferred, and traditional Informal Value Transfer Systems (IVTS) such as hawala and fei qian ('flying money'), which use networks of dealers and a ledger system to move value quickly overseas, also play a role. Another traditional means of transferring value that operates beyond the formal international system – and one that appears to be making something of a comeback – is smuggling cash. In 2024, there have been numerous reported cases of cash couriers being caught smuggling illicit cash using commercial logistics and individual couriers traveling on commercial flights.

Between 2023 and 2024, UK authorities successfully prosecuted and jailed several members of a network that had smuggled Sterling notes worth about $131 million, generated by drug sales, on 83 business class flights from London to Dubai. The funds were packed into suitcases of about $500,000 each.

In June, investigative reporting by UK and Australian newspapers of the News Corp group seemed to suggest that this was but one such scheme amongst many, with the media outlet alleging that British OCGs dealing in drugs were sending millions of pounds in cash to UAE or Africa, in order to purchase illegally mined gold for recast and resale. In a further case from the UK, reported in April, an NCA investigation disrupted an Albanian OCG that smuggled illicit cash to Albania, using a legitimate couriering company as a cover.

While cash is probably still not king when it comes to moving illicit value across borders, in recent years, it appears to have enjoyed something of a renaissance.

Enjoying illicit profits

In the final stage of integration, washed funds are used to buy legitimate items for consumption or investment. This will often include the purchase of high-value goods, such as luxury vehicles, designer clothes and jewelry, redeemable financial products, and – more often than not – property, the purchase of which is widely referred to as 'high-end money laundering.' In its research on the most threatening OCGs in the EU, Europol found that funds were laundered through property in 2/5ths of the networks surveyed.

In the last decade or so, there has been substantial evidence that a large amount of criminal cash has been invested in politically stable European countries and North America. In a report published in May 2024 by several advocacy groups, including GFI, researchers found that at least $2.6 billion in illicit funds, and probably many multiples more, had been used to purchase commercial real estate in the US over the previous two decades, with Florida, California, and New York proving the most attractive locations. Other reports have also suggested the rising importance of other locations, especially those slightly more out of reach for Western law enforcement authorities. Dubai is reportedly one rising destination for high-end laundering, enabled by massive building sprees and encouraged by low taxation rates and a history of troubles with the effective application of AML/CFT measures. While much of this money comes from Western or Russian sources, it is also notable how much money appears to be flowing in from East and Southeast Asia.

Money laundering in 2025

There is no one way to summarize contemporary money laundering. Like many aspects of economic and financial crime, it has become increasingly hybrid. The use of fiat currency sits alongside cryptocurrency. The use of online payment service providers and banks sits alongside TBML, IVTS, and cash couriering. Long-preferred destinations for criminal cash, such as London and New York, have now also been joined by the cities of the emerging markets. Like any complex ecosystem, money laundering continues to evolve. What should we expect from 2025, therefore? Certainly, more of the same, if change can be thought of as 'the new normal.' Money launderers will continue innovating, experimenting, mixing, and matching old methods to beat law enforcement and compliance teams. They will also become more professional, agile, specialized, and transnational in operation.

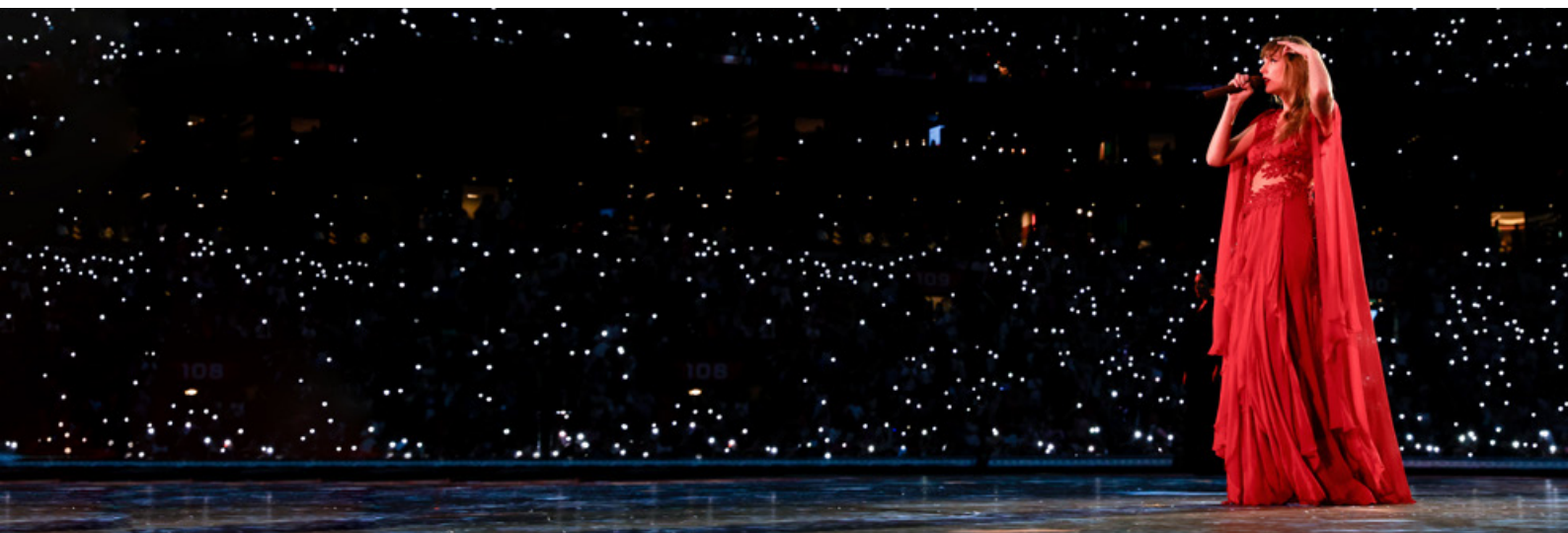
Terrorist financing

Although often discussed in the same breath as money laundering, terrorist financing is a slightly different phenomenon despite using many of the same methods and techniques. The difference between the two is that whereas money launderers wish to hide the source of the funds, terrorist financiers usually wish to hide their destination. In Europe and North America in the early 2020s, the importance of CFT has declined somewhat in relative importance against other financial crime priorities, as groups such as Al Qaeda (AQ) and Islamic State (IS) have suffered operational decline in the West (if not parts of Africa and Asia), and mounted mostly modest attacks conducted by lone actors and small cells, rather than large attacks which require greater organization and funding. Extreme right-wing networks in North America, Europe, Australia, and New Zealand have taken a similar path.

However, in 2023 and 2024, the world has been reminded of the potential impact of Islamist extremist terrorism. In March 2024, IS's Central Asian affiliate, IS-KP, mounted a large-scale attack on a concert in Moscow and was later alleged to have planned a further attack against a Taylor Swift concert in Vienna in August. Other Islamist groups and militias with close ties to Iran – Hamas in Gaza, Hezbollah in Lebanon, and the Houthis in Yemen, the so-called 'Axis of Resistance' – also increased their level of activity following Hamas's massacre and kidnapping of civilians and soldiers in southern Israel in October 2023, and Israel's subsequent military response.

As a consequence, terrorist funding is firmly back as a policy priority for governments and regulators who want to ensure that groups do not exploit the financial system to mount attacks or support wider organizational needs. Considerable attention has focused on the ongoing misuse of the legitimate financial system by well-established groups such as Hezbollah and their allies in the Islamic Revolutionary Guard Corps (IRGC), also proscribed as a terrorist organization in the US, Canada, and a small number of European and Arab jurisdictions. In February 2024, for example, an investigation by Politico, a media outlet, highlighted the role of a small German bank, Varengold Bank AG, which it alleged to be banking IRGC front companies that acted as conduits for sending the proceeds of illicit oil sales to Hezbollah and the Houthis. Politico also suggested that this kind of scheme was also used more widely across the European banking system. A further area of concern has been the exploitation of the European market for high-value goods as a means to store and transfer terrorist funds. In January 2024, the NCA issued an amber alert on art dealing to the sector in the wake of an ongoing investigation of a Hezbollah-linked art dealer based in Lebanon, with paintings stored in the UK worth $1.26 million seized by the authorities.

In addition, there has been renewed interest in 2024 about the potential abuse of crowdfunding as a means for raising terrorist funds. Previous research had indicated that both Islamist extremist groups and the extreme right had attempted to abuse mainstream crowdfunding platforms in the past before moving to the use of dedicated extremist platforms on the Dark Web, or 'pop-up' informal crowdfunding on social media and instant messaging channels. In July 2024, however, Singapore's new Terrorist Financing National Risk Assessment stressed again the important role that crowdfunding could play in terrorist financing, both through fiat currencies and, increasingly, through cryptocurrencies. It noted cases where pro-IS groups in Southeast Asia advertised for donations of crypto online, reports of regular crypto flows to IS-linked individuals in Syria, and a rise in similar activity in support of Hamas after the events of October 2023.



Compliance leaders' perspective on terrorist financing

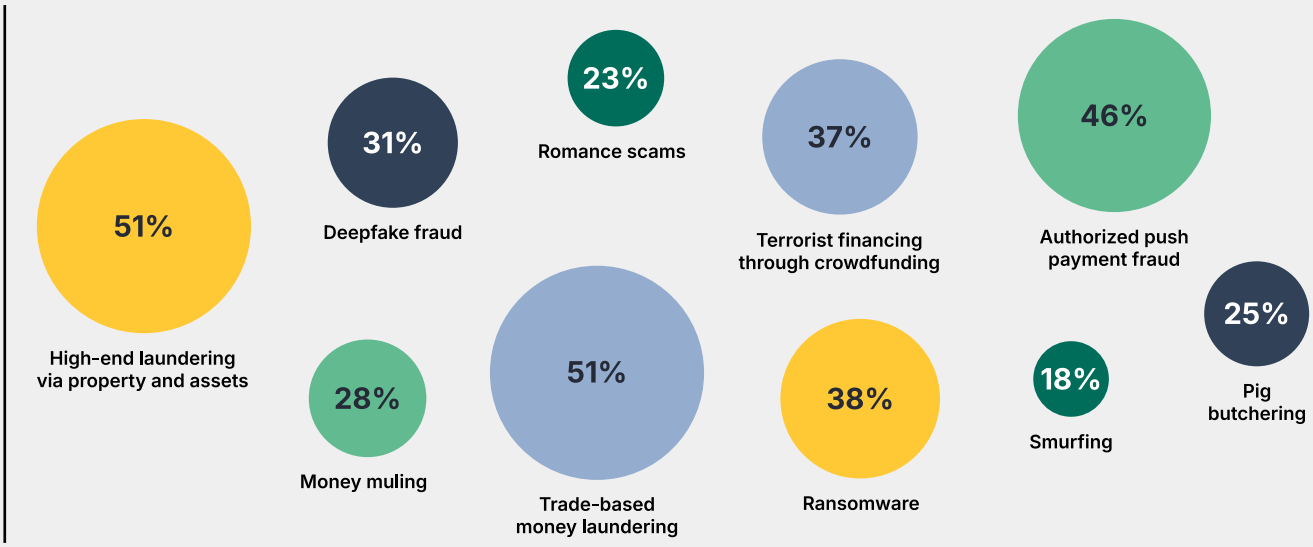
In our survey, respondents showed high concern about several key financial crime typologies. Joint first – at 51 percent – were high-end money laundering, reflecting an ongoing focus on the issue in major developed economies following the passing of the Corporate Transparency Act (CTA) in the US in 2021 and potential sanctions evasion by Russian oligarchs. Also, 51 percent was TBML, which aligned with many compliance teams' concerns about the difficulty of detecting its typologies with current controls. APP fraud came third, at 46 percent, and ransomware fourth, at 38 percent, perhaps reflecting the heavy media and public interest and concern about both, as well as the obvious volume of cases firms have faced. Other issues of concern in the 30–40 percent range included the role of crowdfunding in terrorist financing and the use of GenAI for 'deepfake frauds' – explored in more detail below. These typologies were followed by pig butchering and romance scams, scoring 25 percent and 23 percent, respectively.

What does this mean for me?

- Your team needs to be as agile in its response to money laundering as the criminals themselves have proven to be; they continue to innovate, looking for new methods to move funds and new areas and niches of vulnerability.
- This said, while launderers are using new techniques, they are also combining them with tried-and-tested methods. So, you need to ensure your firm has robust and flexible transaction monitoring platforms available and that they cover the bases of criminal behavior – old and new – as appropriate.
- Your team should also take its exposure to terrorist financing seriously, particularly if you're in an organization that operates on the leading edges of payment services, cryptocurrency, and crowdfunding. But, as with money laundering, you also need to keep your eyes on other more traditional and conventional patterns of terrorist financing, especially for the scale of funds moving through the international system in support of Iran-backed groups.

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

From the list below, what financial crime typologies is your organization concerned about in the next 12 months?



Source: ComplyAdvantage, The State of Financial Crime 2025

Emerging risks

Crypto: The new currency of crime?

It seems strange to highlight crypto – around for well over a decade – as an emerging risk. However, despite dire warnings of the potential for crypto's criminal misuse, the evidence that this has been happening on a grand scale has been less dramatic over the last five to ten years. Although criminals and terrorists have definitely been using crypto, fiat currencies continue to be the main medium of criminal exchange. Evidence from 2024 suggests that this overall balance continues. In Chainalysis's mid-year report, issued in August, the analytics firm found that illicit activity in crypto had dropped just under 20 percent year-on-year and that the legitimate use of crypto was growing at a faster rate than its illicit exploitation. If a crypto-catastrophe has occurred, it has felt more like a small wave and less like a tsunami.

However, while accepting we have not seen a radical pivot to crypto, there is growing evidence that crypto is gaining traction in some criminal areas; indeed, as Chainalysis's own report suggests, within the overall picture of declining illicit usage, there are areas of activity where the use of crypto has risen: ransomware and crypto-hacking. Anecdotal evidence from media reporting also provides evidence which paints an increasingly complex picture. The Asian Racing Federation (ARF) stated in February 2024 that cryptocurrencies were becoming increasingly popular on many unlicensed and illegal betting websites, with some sites providing specific requirements to use stablecoins such as Tether. The ARF's head of research commented that while the world of crypto as a whole was going through "winter," illegal betting with crypto was going through a "perpetual summer." Other reporting from Chainalysis has suggested that cryptocurrency has also become an increasingly common means of buying CSAM, with buyers and sellers using crypto mixers and privacy coins such as Monero to avoid detection.

Crypto has also featured increasingly in varieties of fraud, from well-known founder frauds to lesser-known cases. In June 2024, for example, German and EU authorities disrupted a criminal network that was leasing and subleasing cryptocurrency hardware for mining and exchange, telling investors they would make returns of 70 percent before tax. Instead, the scheme generated losses of 113 million Euros (around $123 million). In August, the FBI highlighted the growing abuse of crypto ATMs by fraudsters, which it believed had been used in scams worth over $120 million in the US in 2023. Overall, the US FTC's data book found that in 2023, payments to scammers were chiefly in fiat bank transfers and payments, at $1.86 billion, but this was followed closely by cryptocurrencies at $1.41 billion.

Most telling, however, has been the growing attraction of crypto to the money laundering business. In Chainalysis's Money Laundering and Cryptocurrency report, published in July 2024, the firm's researchers stated that a rising number of traditional fiat-based money launderers were probably moving into crypto, noting the increase in on-chain behavior of transactional typologies familiar in fiat money laundering. They further noted that these transactions did not appear to be related to known cybercrimes.

The attraction of crypto to traditional money launderers was also increasingly obvious from media reports. In January 2024, for example, the Organized Crime and Corruption Reporting Project (OCCRP), an investigative journalism platform, reported that Brazilian police had disrupted a money laundering operation where drug money worth $2.6 billion had been laundered through the accounts of shell companies, with fiat funds converted into crypto. According to the report, one shell company saw crypto funds worth $285 million pass through its account in just 10 months.

Cryptocurrency has also risen in prominence in the practices of terrorist financiers. In January 2024, the US Department of the Treasury noted in a joint sanctions action with the UK and Australia that since at least 2020, Hamas had been using cryptocurrency to support its operational costs and move value internationally with lower apparent risk. However, Hamas's use of crypto here still seems to be relatively modest; after Hamas's October 7 attack in 2023, The Wall Street Journal claimed that the attacks had been largely funded by crypto. But in the wake of the report, both Chainalysis and another blockchain analytics firm, Elliptic, challenged the paper's claims about the overall scale and importance of Hamas's crypto funding. While cryptocurrency has become more attractive to bad actors in certain areas of criminal activity, it is not yet ubiquitous.

The challenge of generative AI

There has been a great deal of media hype about the positive potential of GenAI – a form of AI that uses deep learning to create text, images, sounds, and other content. Alongside the boosterism, however, there have also been anxieties about its potential misuse, especially in 'deepfakes' used in disinformation campaigns and electoral interference. Across 2024, cases have also emerged suggesting that GenAI is being put to use by criminals, too. At a basic level, criminals have been using GenAI to improve the quality of fake IDs, both for sale on illicit markets and to support their criminal activities. In February 2024, media reports highlighted an online service known as 'OnlyFake,'which was using generative to craft fake IDs for just $15, with images so effective that they could get past several well-known ID recognition platforms. More prominent, though, has been the use of AI in fraud, where INTERPOL noted the increasing use of generative AI tools to conceal real identities, create fake identities, and craft convincing images and voices to confuse victims. In February 2024, Hong Kong police began an investigation into a case where the employee of British engineering firm Arup claimed to have been duped by a deepfake video conference call, where a fraudster, disguised by GenAI as a senior manager of the firm, ordered the employee to make a HK$200 million payment. Other reports from the US suggested that scammers were using deepfakes to contact parents, claiming to be their children, and asking for immediate financial help in a crisis, such as accidents or arrests. In January, cybersecurity firm Resecurity also highlighted the activities of the cybercrime group GXC Team, which announced the development of a generative AI tool, 'googleXcoder,' that could be used to make convincing fraudulent invoices to support BEC fraud.

A further area of law enforcement concern has been the rise of AI-assisted non-consensual pornography. In February 2024, investigative journalism platform Bellingcat reported that G2A, an online video gaming marketplace, was being used to support transactions for Clothoff, one of the major online platforms used to create deepfake non-consensual pornography. While this case appeared to have involved adult images, Europol also highlighted in July the growing danger that GenAI would be used to create CSAM.

Emerging risks in 2025

Balance is always required when assessing the likely impact of new technologies on criminal behavior.
It can be tempting to assume the worst or, in contrast, be underwhelmed by their immediate impact. However, the exploitation of technology needs to be considered over an extended period; sometimes, new technologies catch on straightaway, but more often, they only become widely employed when a critical mass of use cases emerge.
Therefore, it should be no surprise that the criminal exploitation of crypto has been more of a slow burn.
Crypto is not inherently criminal, but it is increasingly used in particular fields of criminality. The use of crypto by fraudsters and money launderers seems likely to accelerate in 2025 and beyond, especially if governments and regulators continue to play catch-up on creating a flexible and up-to-date AML/CFT framework for the sector.
With regard to GenAI, by contrast, we are at a much earlier stage of the cycle. 2025 is likely to see more criminal usage of deepfakes - and even less accomplished 'cheap fakes' – for fraud, but as businesses and individuals become more aware, its effects are likely to be blunted. That said, over time, the technology will probably improve, suggesting that GenAI is likely to be a much more difficult challenge in the medium-to-long term.

What does this mean for me?

- If your firm is operating in or exposed to crypto, you should take its potential for exploitation seriously. Given its growing ubiquity in certain aspects of economic and financial crime, your team can not simply shrug off the risks as an overreaction of regulators or the mainstream financial system. You, therefore, need to deploy appropriate AML/CFT measures – robust due diligence, monitoring, and screening – to protect not only your businesses but also the long-term reputation and credibility of the sector. Crypto has much to offer, and this should not be sacrificed out of an unwillingness to take appropriate precautionary measures

- GenAI will be a long-term and thorny problem for a regulated sector that depends so much on identifying and verifying individuals to sustain business. This said, it is not quite yet time to panic, as the quality of GenAI content has varied widely. With increased awareness of the potential for its misuse and the advance of digital ID, which is itself informed by AI, the worst effects will be limited for now. You, therefore, need to ensure you raise the awareness of your customer base about the potential criminal abuse of AI and that a full suite of financial crime controls is in place to supplement identification and verification (ID&V) platforms. However, you also need to keep a close eye on how GenAI develops and improves over time.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

Regional trends

United States

The experience of the United States in 2024 has been broadly reflective of the wider trends outlined in this chapter.

In February, the US Treasury issued its latest National Risk Assessments on Money Laundering, Terrorist Financing, and Proliferation Financing, which found that the most significant illicit flows in and/or through the US came from fraud, illegal narcotics, cybercrime, human trafficking, illegal migration, and corruption. The reports also highlighted the important role that organized crime played in most of these areas, with a particular focus on Mexican cartels.

The cartels have shown a willingness to innovate and diversify. The investigative media outlet the International Consortium of Investigative Journalists (ICIJ), noted in May that over recent years, they have become more involved in the smuggling of migrants over the US border, replacing the much looser and less efficient networks of smugglers known as 'coyotes' or 'pelleros,' and enabling a much higher volume of illegal migrants to enter the US. The cartels have also shown a willingness and capacity to innovate in their core trade of illegal narcotics, especially in boosting the production and supply of synthetic opioids. Here, the US Treasury's reports highlighted the role of two Mexican cartels – Sinaloa and the Cartel Jalisco Nueva Generación (CJNG). Both have played major roles in the development of industrial-scale fentanyl production in Mexico and its export to the US and Canada.

According to the US Treasury, one of the most important aspects of the growing Mexican production of synthetic drugs has been the relationship between Mexican cartels and Chinese OCGs. Initially, much of the trans-Pacific cooperation between different groups focused largely on the supply of precursor chemicals that are used in the production of various drugs, including synthetic opioids. In April 2024, The Economist noted this tightening bond, as Chinese money launderers replaced native Mexican groups because of the relative cheapness of their operations and the flexibility of the 'flying money' system, which is both opaque and hungry for US dollars to exchange for yuan. According to the US DHS, Chinese money launderers have thus become "key cogs in the multi-billion-dollar criminal empires run by Mexican cartels and other transnational criminal organizations."

Chinese OCGs have also expanded their operations in other areas of criminal activity within the US itself. Reporting in April 2024 from ProPublica, an investigative journalism platform, noted that Chinese OCGs, already the major players in the illegal marijuana market in the US, had expanded their activities into massive fraud schemes, particularly through 'card draining' of gift cards stolen from major chains such as Walmart and Target. According to the report, US authorities believed such schemes would likely generate hundreds of millions of dollars for Chinese OCGs.

Europe

Across Europe, organized crime has also continued to evolve in 2024. As noted previously, Europol issued a report in April analyzing the highest-risk OCGs operating within the EU.

Much like in the US, the core activities of European organized crime include illegal drugs, fraud, migrant smuggling, and human trafficking.

However, as Europol notes, there are increasing instances of poly criminality, with OCGs diversifying across various crime types.

One of the interesting similarities between North America and Europe is the increasing role of organized crime in migrant smuggling. According to a separate Europol report by the agency's European Migrant Smuggling Centre (EMSC), published in July 2024, investigations revealed that migrant smuggling groups were also involved in other activities, such as drugs, human and arms trafficking, and fraud.

European authorities have also found growing patterns of international cooperation between European groups and networks from other regions. In September, for example, Italian police disrupted a drug trafficking network involving both Latin American and Albanian OCGs, whose money laundering needs were served by Chinese money launderers.

However, there are some variations in the US. Although the US has a buoyant demand and supply of cocaine and illegal cannabis, in recent years, North America has been a growth area for synthetic opioids.

In contrast, Europe is still heavily dominated by cannabis, cocaine, and methamphetamine. According to the EU Drug Markets Analysis 2024, published by Europol and the European Monitoring Center for Drugs and Drug Addiction (EMCDDA) in March, cannabis remains the most used illegal drug in Europe, followed some distance behind by cocaine. However, the agencies note there has also been a "significant cocaine influx from Latin America" despite several successful police raids on cocaine supplies across Europe. In a wastewater analysis published in March, the EMCDDA found the same concentrations of South American cocaine and methamphetamine in water consumed in small towns as in European cities and large towns, eliminating a differential between different types of residential areas that had long existed. Part of the continued success of cocaine in Europe seems to be the result of OCG innovation. Rather than continue using traditional destinations such as the ports in the low countries and Germany, OCGs have turned to less busy ports in the UK, Scandinavia, and Russia. There have also been indications, according to the EMCDDA, that some European OCGs have switched from importing processed cocaine to intermediate products such as coca paste and cocaine base, which can then be prepared in Europe.

In contrast to the US, the European opioid market continues to be primarily dominated by heroin. In January 2024, in a joint report on opioids, Europol and EMCDDA noted that the retail heroin market in the EU was worth at least €5.2 billion annually (over $5 and a half billion), with no signs of shortages, despite the Taliban's 2022 ban on poppy cultivation. However, both agencies have noted that certain synthetic opioids and other substances that might be used as replacements for heroin have started to develop footholds in European markets. In a separate report issued in June, EMCDDA noted an uptick in the use of veterinary tranquilizers and a rise in deaths from nitazenes in some Baltic states, France and Ireland.

Beyond the core predicate crimes of organized crime, Europe also faced a rising incidence of particular types of public sector fraud. In March 2024, the European Public Prosecutor's Office's (EPPO) annual report for 2023 revealed how EU funds were becoming major targets, noting that, out of 1,927 investigations, 206 had looked at frauds perpetrated in projects funded by NextGenerationEU, the EU's initiative to support economic recovery after the pandemic, and the transition to green technologies.

Between them, these 200 or more frauds led to losses exceeding €1.8 billion (just under $2 billion), around 25 percent of all EU funds lost through fraud.

Numerous examples of alleged cases were reported throughout 2024, including investigations into a Lithuanian firm developing biodegradable cling film, an Italian winery being converted to organic farming, a Romanian strawberry and lettuce farm, and a Bulgarian chicken farm.

Another growing area of fraudulent activity in Europe in 2024 has been a growth in fraud around the European sales tax, Value Added Tax (VAT).

Involving schemes of varying degrees of complexity, VAT fraud ultimately aims to siphon off the value of the tax paid during trade within the EU. Cases that emerged throughout 2024 include a car trading scam based in Germany, a wine-based fraud centered in Italy, and a further case centered in Germany that defrauded authorities out of €195 million (around $212 million) from the sale of electronic devices such as smartphones.

While many public funds and tax frauds appear to have been run by one-off criminal conspiracies, there is also evidence to suggest that organized crime has a hand in these schemes, too. In testimony to the anti-mafia commission of the Italian Chamber in July 2024, Enzo Serata, director of the national financial intelligence unit (UIF), noted how Italian OCGs had penetrated several aspects of the renewable energy sector – a potent source of public funds – including the redevelopment of agricultural land and the building of new power plants. The EPPO has also raised similar concerns about organized crime's role in VAT fraud in its 2023 annual report, stating that of the €19.2 billion stolen from the EU budget by organized crime (just over $20 billion), approximately €11.5 billion ($12.5 billion) – 59 percent – came from VAT fraud. It seemed that, as with organized criminality throughout the world, European OCGs have also continued to find ways to penetrate and exploit not only illicit fields of activity but the most vulnerable, too.

Asia-Pacific

Both the US and Europe have witnessed the growing presence of Chinese organized crime and money laundering operations in 2024.

However, Southeast Asia is the region where this has been most strongly felt, where many Chinese criminal groups have made their bases.

According to a study published in May 2024 by the US Institute of Peace (USIP), a think tank, syndicates based in the region generated illicit proceeds of $64 billion worldwide in 2023 alone. Given the increasing global spread of Chinese OCGs, it seems likely that a significant proportion of these funds are laundered widely across major global financial centers and jurisdictions closer to home. Throughout 2023 and 2024, for example, authorities in Singapore provided updates on a major money laundering investigation, which led to the freezing or seizure of worth over S$3 billion (c.$2.2 billion).

Several individuals held passports from third countries, such as Cambodia and Cyprus, but appeared to be of Chinese origin.

A crucial element in the current success of Chinese criminal groups is their involvement in the nexus between human trafficking, cybercrime, and online scams: the previously highlighted 'scam centers.' Although such centers have emerged worldwide, remote and poorly policed border areas in Myanmar, Cambodia, Vietnam, Laos, and Thailand have been the homes of the largest concentration. UN estimates suggest that around 120,000 trafficked victims are held in scam centers in Myanmar alone, with a further 100,000 in Cambodia and other countries in the region. These centers, often based alongside illegal, unlicensed casinos, use trafficking victims to conduct frauds and scams, work in illegal online betting platforms, and support money laundering activities through crypto exchanges. In an investigation from January 2024 by the media outlet Deutsche Welle (DW), journalists met survivors from one compound in Myanmar who described a life of constant surveillance, torture, and murder, with 17-hour working days and limited rest. The DW investigation also found links between the compound and Chinese front companies, which are alleged to be part of the criminal empire of Chinese criminal kingpin Wan Kuok Koi, or 'Broken Tooth.'

Chinese and other regional OCGs have continued to operate in the illegal narcotics market, cooperating, as previously noted, with groups in the Americas and Europe. They have also worked to expand the Asian market for drugs, importing increasing amounts of cocaine from Latin American partners that flows into China, India, and South Korea. The UNODC has also reported increasing flows of methamphetamine into the region, with a June 2024 report by the agency noting that 190 tons of the drug had been seized by authorities in Southeast and Asia in 2023, an annual record. At the same time, the region's OCGs have sought to diversify into less obvious areas of criminal activity, much as their counterparts in the Americas and Europe have done, including into environmental crimes such as illegal wildlife trafficking and illegal mining.
A related area of growing criminal activity in Southeast Asia, noted by the UNODC in April 2024, is the black market in illegal waste dumping operations, with the region serving as the destination for increasing inflows of illegal waste from the EU. Not only are OCGs making the region a hub of illicit activity, but they are potentially toxic, too.

Regional trends in 2025

The regional development of organized, financial, and economic crime in 2025 depends on numerous variables, many of which relate to the ongoing openness of the world economy and the broader global geopolitical context. If the world becomes more fragmented and unstable in 2025 – a reasonable possibility – then criminals will probably face new challenges initially. Still, experience suggests they will quickly regroup, innovate, and find new ways to make money. OCGs are extremophiles – organisms that can thrive in the most inhospitable environments. Within individual regions, observers should look out for the following:

- **US/The Americas:** The diversification of Latin American cartels' operations and their growing convergence with Chinese networks is likely to continue in all foreseeable circumstances. Organized criminality and the economic and financial crimes that flow from it will thus continue at a high level in the US and its neighbors in 2025. The Trump administration will attempt to undermine those aspects of organized criminality that touch on the president's key political themes; these will include stronger border controls, deportations of illegal immigrants, and more kinetic actions against criminal activity along the US-Mexico border. Legal challenges and diplomatic complaints will blunt the edges of some of these actions, but it is unlikely that the Trump administration will be easily diverted. However, the effectiveness of these measures remains far from certain.
- **Europe:** European organized crime will continue to operate at scale, relying on a massive demand for its services, especially in the market for cocaine. Foreseeable problems such as a heroin shortage are likely to be easily made up for with synthetic alternatives. However, there are no immediate indications of a US-style epidemic of synthetic opioid usage. European OCGs will also continue to explore easy-to-access, low-risk, low-cost endeavors such as VAT and public funds fraud.
- **Asia-Pacific:** Southeast Asia will remain the epicenter of a growing ecosystem of transnational criminality that traces its roots back to China. These OCGs will continue to use this part of Asia as a relatively untouchable base while targeting victims both in the region and further afield. Online scamming and illegal betting have proven to be major money-spinners and will likely remain a major focus. Asian OCGs are also likely to work hard to open up a wider market for various illicit narcotics in the region. Although the Trump administration is likely to put significant diplomatic pressure on China to disrupt the flow of narcotic precursors from Asia to the Americas, Chinese government efforts are likely to be half-hearted, and their impact is limited at best.

What does this mean for me?

- The overall picture of criminal activity globally and in the regions is far from positive. In an increasingly fractious and fragmented world, there is every reason to expect that criminals will be able to take advantage, and governments and their agencies will struggle to keep up.
- So, it is more important than ever for your team to take its compliance and financial crime risk management responsibilities seriously. While the regulated sector is not directly responsible for defeating crime, it undoubtedly has the responsibility of helping insulate the financial system from bad actors, protecting customers, and identifying and reporting potential criminal actors.
- To achieve this, you need to look closely at the range of risks your firm faces – from specific predicate offenses to money laundering and terrorist financing. You need to internalize and understand those risks and act accordingly, using reliable risk data and agile platforms. It is not enough for your organization to spend money on compliance systems. To have a real impact, you need to spend it wisely.

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

Back to beginning
Previous section
Next section

Geopolitics and sanctions

2024: Elections, instability and war

2024 was a remarkable geopolitical year. It was, for one, a year of elections, with over 1.5 billion voting in over 50 countries, including Taiwan, South Africa, Russia, India, the UK, and, of course, the US. Several of the results fell largely in line with expectations: Lai Ching-te, the Democratic Progressive Party (DPP) candidate for president in Taiwan, defeated his nearest opponent by a comfortable margin in January, and in July, Labour beat the Conservatives in a landslide in the UK. Vladimir Putin was re-elected president of Russia in March for another six-year term.

Other results were more surprising. In June, the Bharatiya Janata Party (BJP), led by Narendra Modi, was returned as the single largest party in India's elections. At the same time, however, it lost its parliamentary majority, denting Modi's 'strongman' image. Another unexpected result came in June when France's President Emmanuel Macron called early elections for the National Assembly. Gambling that a new assembly would give him greater political latitude, he was instead faced with a victory for Marine le Pen's far-right National Rally (RN), which won the most seats, if not a majority. Other parties of the far or populist right did well in Europe, too, making advances in the European Parliamentary elections, which also took place in June, and in German state elections in September. The results seemed to suggest an atmosphere of discontent and uncertainty in Europe, which was further evidenced in November when German Chancellor Olaf Scholz's Ampelkoalition (traffic light coalition) collapsed. A federal election will take place on February 23, 2025.

The most consequential election result of 2024, however, was the US presidential election. The relatively comfortable re-election of Donald Trump in November – who won both the electoral college and the popular vote – was a surprise to many observers. With the replacement of President Joe Biden by Vice President Kamala Harris as the Democratic candidate in August, many expected a tighter race or even a narrow Harris win, but in the end, generational change proved insufficient to save the Democrats. Indeed, the Republican Party stood in a position of rare power in the US by the end of the year, having won both the Senate and House of Representatives as well.

Although many had feared civil disturbances in the wake of the election, violence did not ensue.

Elsewhere, however, there was unexpected political instability. In August, Sheikh Hasina, the leader of Bangladesh, was forced to resign by sustained protests, robbing Modi of a strong regional ally. Elsewhere in Asia, apparently stable democracies seemed to wobble; in December, South Korean President Yoon Suk Yeol sought to impose martial law in the face of a legislative impasse but was forced to rescind the measure by parliamentary action and public protests.

2024 also proved to be a year of ongoing war. Russia's war on Ukraine continued despite limited gains for both sides. Israel's war against Hamas continued, too, and briefly threatened to flare into a regional conflict when Israel took on Hamas's allies in Lebanon, Yemen, and Iran. Forgotten wars – in Sudan, for example – also regained some international attention. Syria returned to the headlines in December when an anti-Assad group, led by Islamists, took the Syrian cities of Aleppo and Hama before heading south to Damascus and overthrowing the Assad regime.

2025 in prospect

The inauguration of Trump in January 2025, supported by a diverse array of idiosyncratic senior appointees such as Elon Musk and Robert F. Kennedy Jr., is likely to lead to a period of significant domestic change in the US and the wider world. One of the most certain effects will be economic. If Trump brings forward his proposed raft of trade tariffs on opponents and allies alike, a trade war is likely to cause a significant drag on global growth.

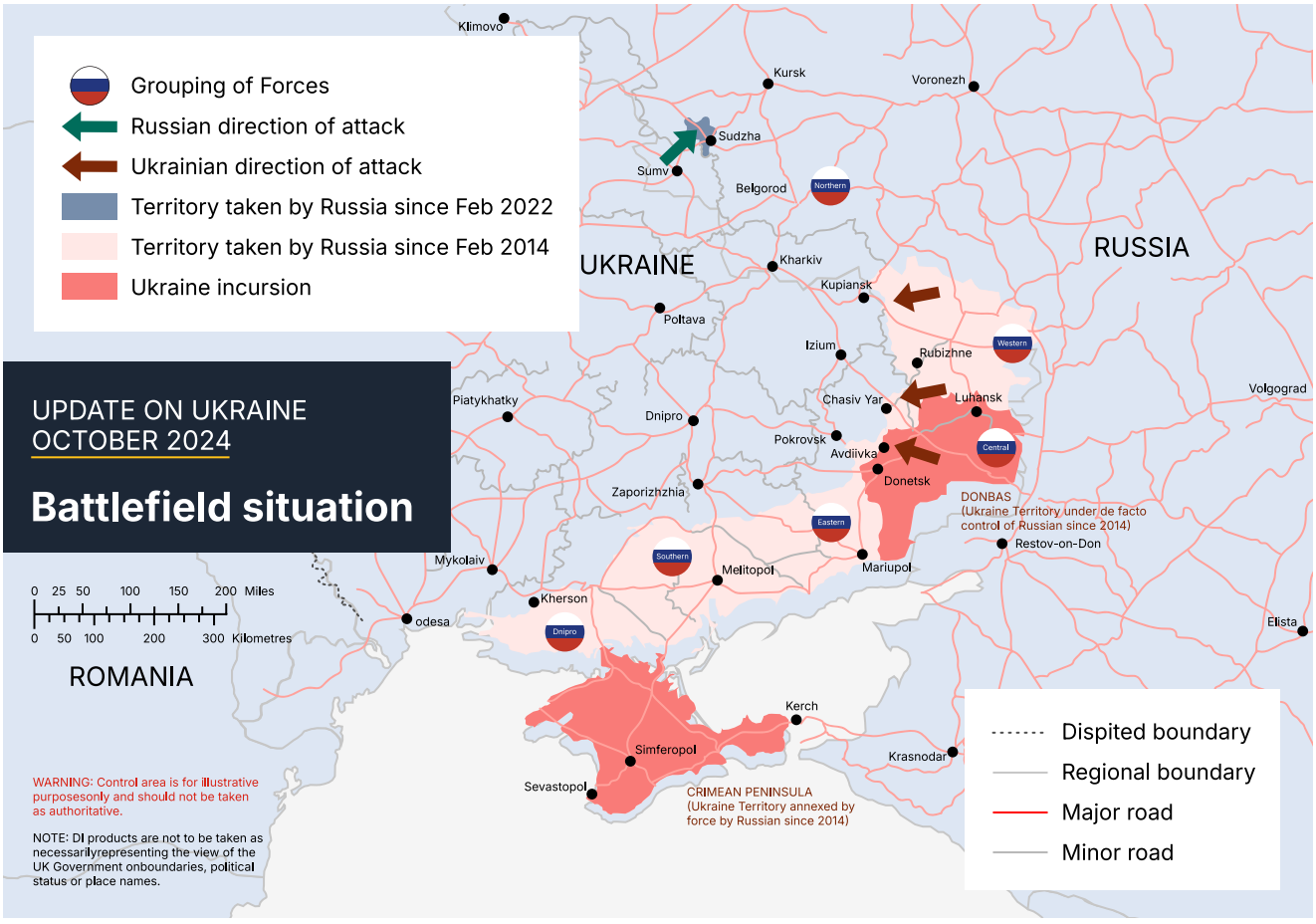
A further shockwave is likely to come from Trump's threats to use the US military to deport illegal migrants over the US-Mexico border. The US itself will face a tightening labor market, driving up prices and undermining growth. Latin American countries will face substantial disruption, too; with the growth of camps of deported or blocked migrants, there is likely to be unrest in local communities and potential border disturbances that could involve US and Mexican agencies as well as the cartels. The more difficult the border crossing into the US becomes, the more business there will also be for the most sophisticated and innovative smugglers.

Trump's return will also affect ongoing geopolitical fault lines in Europe, the Middle East, and Asia-Pacific. 2025 is likely to be a difficult period for the US's allies, with the new president emphasizing the need for them to pay for their own defense – or else. Moreover, while starting with apparently warm words for the leadership skills of Putin, Xi Jinping of China, and Kim Jong-un of North Korea, how he will handle practical relations with these countries seems far from certain. Given Trump's mercurial character and depending on the turn of events, either rapprochement or confrontation could follow. A hard-line stance is likeliest with China, which the incoming president sees as the greatest economic threat to the US, but he has also taken a tough approach to Iran, providing strident support of Israel's actions against Hamas, Hezbollah, and Iran since the October 7 massacre in 2023.

In this unpredictable environment, Russia, China, North Korea, Iran, and others are likely to tread warily, seeking to flatter the incoming president and encourage his deal-making instincts while driving wedges between the US and its allies. At the same time, these revisionist countries – unhappy with the Western rules-based international order – are also likely to come closer together, especially economically and financially. Military and security cooperation between Russia and North Korea and Russia and Iran will also increase, but China will likely remain cool on becoming too heavily involved in a military face-off with the US, at least for the time being. However, unexpected developments might take matters out of Beijing's control, and there is the added risk that a tightening revisionist alliance, which the US perceives to be against its interests, might yet provoke Trump to take a more hostile stance towards it. If it does, then economic and financial sanctions are likely to be among the first tools for which the US will reach.

The War in Ukraine

Under President Putin, Russia has become among the world's most dangerous troublemakers, backed up by economic resources, significant armed forces, and a massive, increasingly sophisticated nuclear arsenal. In its first decade, his regime was careful to avoid confrontation with the West, although tensions emerged over Russia's treatment of dissidents, critics, and whistle-blowers, such as Sergei Magnitsky, a Russian accountant who died in Russian custody in November 2009 after revealing a fraud by state officials. In its second decade onward, however, the Putin regime has become much more willing to take on the West directly, and a major crisis in relations occurred in March 2014, when Russia illegally annexed the Ukrainian region of Crimea and increased its support for Ukrainian separatists fighting against the Kyiv government in the east of the country. Since 2014, the Russian relationship with Western governments has deteriorated further, prompted by aggressive Russian actions such as the attempted murder of former Russian intelligence officer Sergei Skripal in the UK in 2018. The final breach came in February 2022 with Russia's full-scale invasion of Ukraine, when the Russian army sought, unsuccessfully, to overthrow a Ukrainian government it believed was becoming too close to the West. This led to what German Chancellor Olaf Scholz described as a "zeitenwende" for Germany, or a historic point in relations with Russia, which was paralleled by a decisive turn against Moscow in capitals across the West.



Source: UK House of Lords

The US and its allies responded to the invasion with substantial military and humanitarian aid to Ukraine, an unprecedented set of peacetime sanctions on Russia and its non-combatant ally, Belarus. Given its scale and breadth, the sanctions regime against Russia cannot be explored in full detail here, but key elements have included:

- **Personal sanctions** on major Russian political, economic, military, and media figures involved in executing and enabling the invasion and the Putin regime, including Putin and his wealthy oligarch supporters.

- **The freezing of Russian state assets** including around $350 billion in foreign currency reserves, the freezing of major Russian private bank assets, and the removal of major Russian banks from the SWIFT international payments messaging system.

- **Export bans** on weaponry, dual-use items, and high technology that could be used to support the Russian war effort.

- **A range of import bans and controls** on key Russian commodities such as hydrocarbons, metals, and minerals. One of the most significant controls, introduced in December 2022, has been the G7 ban on trade in Russian oil above the price of $60 a barrel. This while allowing Russia to continue to trade with non-sanctioning jurisdictions, is intended to reduce Russian oil profits.

This post-invasion sanctions regime was built on a number of pre-existing measures that had mostly, but not exclusively, been imposed by the US. These targeted individuals and entities involved in the 2014 war against Ukraine and the annexation of Crimea, Russia's electoral interference in the US in 2016, cyberattacks against the US government, businesses, and infrastructure, assassinations overseas, and the regime's corruption and domestic abuse of human rights. This included the maltreatment of the aforementioned Sergei Magnitsky, in whose name the US and several other Western states, including Canada and the UK, created dedicated sanctions regimes to promote human rights. Although not often referred to in discussions of sanctions against Russia, these types of sanctions have also increased in number and range throughout the war in Ukraine as a complement to measures aimed more directly at the Russian war effort itself.

2024

No end in sight?

On November 19, 2024, the war in Ukraine reached its one-thousandth day. Despite Trump's promise to end the war within 24-hour hours if re-elected, and rising hopes for some form of early negotiation – President Volodymyr Zelensky of Ukraine stated the war would end "sooner" as a result of Trump's arrival – no immediate end to the war was in sight at the end of 2024.

In many ways, the overall situation in 2024 broadly matched what was foreseen in last year's State of Financial Crime 2024 report, where we suggested a further year of military stalemate and attrition, with few major military breakthroughs. We also noted increasing pressure on both Ukraine and Russia to begin negotiations and saw talks as possible but unlikely. Militarily, this assessment has proved broadly correct for most of the year, although, in the autumn of 2024, Russia began to make small but sustained advances in the south and the Donbas region in the east, with its army making its largest monthly gains since the first full month of the war in October. Russia has also been able to sustain major drone attacks against Ukraine's critical national infrastructure, energy supplies, and civilians.

Major reasons for the gradual Russian battlefield successes have been the growing differential in Russian and Ukrainian manpower numbers and the episodic and sluggish aid pipeline from the US and its allies in Europe, exemplified by the US Congress taking six months to pass a bill including $61 billion for Ukraine in April 2024. Both have worn down the Ukrainian army's basic capabilities, but more importantly its morale and, arguably, that of its citizenry. Russia has also been helped by a still-growing economy, strong trade in sanctioned goods such as oil and gas with non-Western countries, and direct military assistance from Iran and, increasingly, North Korea. Indeed, North Korean aid increased dramatically in October, when around 10,000 North Korean troops were deployed to Russia to fight alongside the Russian army.

Nonetheless, President Putin did not have matters all his own way in 2024. The Russian army has achieved small territorial advances with a dramatic cost in lives. In November, UK officials estimated that in the preceding month, Russia had lost around 1500 men a day, amounting to around 46,000 in total.

This is a staggering figure, especially when one considers that the Soviet army lost around 15,000 in ten years in Afghanistan between 1979 and 1989. Russia also suffered the major embarrassment of losing substantial amounts of territory around Kursk in August, when Ukrainian forces took advantage of thin Russian lines in the north to launch a major incursion. Despite repeated Russian counter-attacks, Ukrainian forces managed to retain a foothold.

A further blow to Russia came in November when President Joe Biden agreed to let Ukraine use long-range, US-supplied ATACMS missiles on targets inside Russia. This was a development that Putin had long warned against, saying that it would make NATO countries co-combatants in the war and incur potential retaliation (including a possible tactical nuclear response). In November, Putin underlined this threat further, lowering the thresholds for using nuclear weapons on the same day that Ukraine used US missiles for long-range strikes inside Russia. However, battlefield nuclear weapons were not introduced, although a new hypersonic ballistic missile with nuclear capabilities was used against Ukraine instead.

More Western sanctions

Several of the major players in the development of the sanctions regime against Russia – in particular the US, EU, and UK – have continued to expand and tighten existing measures in 2024. Much of this activity has been co-ordinated, although each sanctioning authority has retained its discretion and there continues to be significant variety between the different national regimes. For all the sanctioning powers, however, one of the primary concerns throughout 2024 has been to find ways to help sanctions work better and reduce loopholes for evasion.

United States

In February, the Biden administration marked the second anniversary of the full-scale Russian invasion of Ukraine with a raft of over 500 new sanctions, the largest up to that point. The package had several key themes. Russian access to the international financial system remained a primary concern, with the US designating several regional Russian banks, investment funds, and the National Payment Card System.

Another key issue addressed was the circumvention of Russian sanctions. The US continued to apply new secondary sanctions – measures prohibiting engagement with third-country businesses and individuals doing business with primary targets – to over two dozen companies based in China, several European countries, Central Asia, the Middle East, and Southeast Asia. It also added over 90 firms in third countries to the Department of Commerce's 'Entity List,' making them subject to US export restrictions. Other key areas of activity in the February package included targeting advanced technology used in Russian arms production, oil shipping and logistics, and the Russian diamond and gold trades. These areas were revisited in further rounds of action throughout the year.

In the financial sphere, the Office of Foreign Assets Control (OFAC) targeted Russian FinTechs, such as B-Crypto and Masterchain, which it claimed had helped sanctioned Russian banks to make payments using crypto and digital assets. More traditional financial avenues were also addressed. In June, OFAC sanctioned the Moscow Exchange and extended its legal definition of the Russian "military-industrial base" to include major banks such as Sberbank and VTB, allowing the US to level secondary sanctions against third-party entities that did business with them. OFAC increased the pressure on Russian financial services in late November, designating Gazprombank, one of Russia's largest banks and intimately involved in its hydrocarbon trade, as well as 50 other Russian banks with international links.

The US also continued to target sanctions workarounds involving Russia's partners in Iran and North Korea, as well as companies in third countries that had continued to trade with Russia despite Western measures. These designations included over 400 sanctions in August, which targeted Russian and third-country firms in the defense and technology sectors, as well as a September designation of a Russian-North Korean evasion network hat involved several Russian banks operating through South Ossetia, a Russian-occupied region of Georgia. A further 400 designations of entities in Russia and third countries, including India, China, Türkiye, and UAE, came in October. The evasion methods of Russia's oligarchs were also targeted in May when OFAC designated Dmitrii Beloglazov and several of his companies in an effort to help sanctioned oligarch Oleg Deripaska sell shares worth $1.5 billion.

The Russian metals, minerals, and mining industries were a further ongoing focus of the US. In April, the Senate voted to ban the import of Russian uranium, and the US government banned the imports of Russian aluminum, copper, and nickel, with the Chicago Mercantile Exchange ending trade in these items too. Further businesses in the steel, iron and coal mining industries were designated in August.

European Union

In tandem with the US, the EU put forward wide-ranging packages of restrictive measures against Russia and Belarus in 2024 – the 13th and 14th – in February and June, respectively. In its February package, the EU continued to designate entities and individuals linked to Russia's military and industrial war effort, as well as Russian officials involved in the management of occupied areas and
abuses such as the transfer and deportation of Ukrainian children. As with US measures, the EU also paid major attention to the issue of third-country support for Russia. Russian businesses and individuals involved in the procurement and supply of North Korean weapons and munitions were designated, as were several North Korean and Belarusian targets, including North Korea's defense minister. This package also imposed restrictions on the export of dual-use technology used in the manufacture and deployment of military drones, targeting specific companies in operating countries being used as back-channels, including China, India, Serbia, Türkiye, Kazakhstan, Thailand, and Sri Lanka.

In its June package, EU efforts to tackle Russia's procurement of dual-use goods continued, extending export restrictions to items including microwave amplifiers and all-terrain vehicles, as well as some industrial plastics, chemicals, metals, parts, and machinery. Over 60 entities involved in the supply of dual-use goods, both in Russia and third countries were also listed. Alongside these measures, the EU made efforts to tighten energy-related sanctions, prohibiting engagement with current and future Liquid Natural Gas (LNG) projects in Russia and scheduling the prohibition of the transshipment of Russian LNG by European ports in early 2025. The EU also targeted Putin's 'shadow fleet,' designating specific tankers used to transport military equipment, stolen Ukrainian grain, LNG, and oil sold above the price cap. Further measures in the 14th package included a ban on banks using the Russian transaction messaging system, SPFS, an alternative to SWIFT, and on transactions with banks and crypto asset service providers in Russia and third countries that are involved in supporting the Russian military-industrial complex.

The EU introduced other specific measures throughout the year, including the suspension of broadcasting by several Russia-linked media platforms and the sanctioning of one – Voice of Europe and associated individuals, Artem Marchevskyi and Viktor Medvedchuk. The EU also

implemented tougher measures to deter Iranian support for Russia, listing more Iranian firms and individuals involved in the supply of drones and missiles to Russian forces. In June, the EU also took action that corresponded with US actions against Russian businessman Dmitrii Beloglazov, sanctioning both him and his firms for involvement in the planned Deripaska share sale scheme.

The UK and other national regimes

Beyond the US and EU, the most active sanctioning jurisdiction in 2024 was the UK, which took various measures that mirrored both of its allies. In February, firms and individuals involved in Russian munitions manufacture, machine tool trading, and diamond production were targeted. In April, the London Metal Exchange blocked transactions related to aluminum, copper, and nickel produced by Russia. In June and September, the UK also focused on the Russian 'shadow fleet,' designating vessels used in sanctions circumvention around the oil and LNG trade and targeting Ingosstrakh Insurance, which has provided insurance cover for the shadow fleet's activities. In October, moreover, the UK imposed measures against Russia's state-funded public relations agency, the Social Design Agency (SDA), and partner agencies for undertaking subversive activities in Ukraine. The UK also sought to expand its range of powers to tackle sanctions circumvention in July, amending its regulations to allow the designation of third-country companies and individuals providing financial services in support of the Russian war effort.

Other countries took additional measures. Switzerland, for example, continued to largely mirror the measures taken by the EU, but with some exceptions for Russian subsidiaries operating in the country. Both Japan and South Korea have continued to extend their regimes and have been particularly concerned by the growing scale of North Korean support for the Russian war effort. In May, Japan imposed new measures targeting Russian weapons procurement from North Korea, channeled through companies in Cyprus, and South Korea listed two Russian ships used in sanctioned North Korea-Russia trade, and several North Korean individuals involved. Canada also extended measures throughout the year, targeting Russia's diamond trade, North Korean and Iranian support for the Russian war effort, and sanctions circumvention.

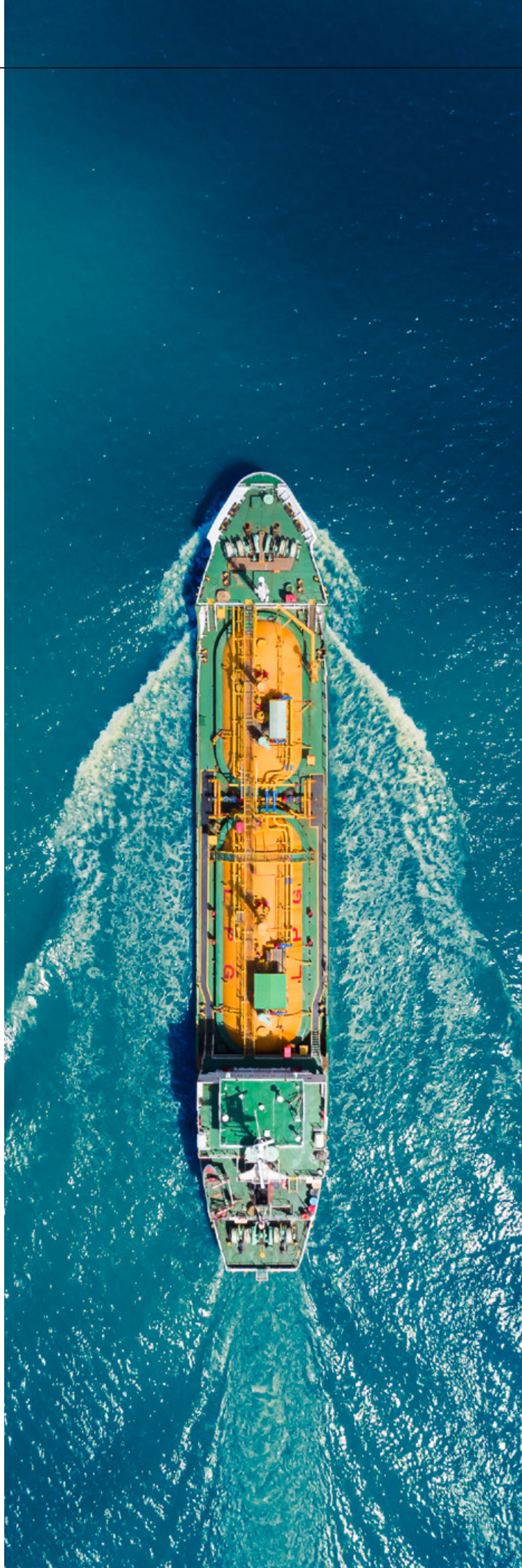
However, some countries with existing sanctions against Russia, such as Australia and Singapore, made no major extensions in 2024, and those states which had not imposed sanctions of their own – China, India, and Türkiye, for example – continued to try to balance business with Russia and the West. Although the core Western countries have remained resolute in their approach, there was a definite sense that beyond the core sanctioning jurisdictions, the appetite for more sanctions was limited.

Making sanctions stick, making Russia pay

Making designations was only one aspect of the Western sanctions' effort. Trying to ensure their effectiveness was another. Diplomacy, both public and private, was one ongoing avenue for applying pressure to ensure compliance. Third countries such as UAE, India, and Türkiye were subject to repeated US requests to suppress sanctions evasion through their economies and financial systems, and in April, US Secretary of State Anthony Blinken warned China about its businesses' support for the Russian defense sector.

However, direct enforcement was also an important tool in 2024. Those suspected of involvement in active sanctions evasion were subject to investigations in North America and Europe, leading to several legal actions. In January, the UK's National Crime Agency (NCA) arrested Dmitry Ovsyannikov, a former official in occupied Crimea, on suspicion of sanctions-related crimes and money laundering, making him the first person to be arrested for Russian sanctions evasion in the UK. Western authorities also sought to use regulatory measures to tackle breaches by the private sector. In July, Lithuanian authorities fined Payeer, a cryptoasset service provider, the equivalent of just over $10 million for AML/CFT failures around Russian sanctions.

New sanctions and enforcement measures clearly had a persuasive impact in some areas, such as the logistics sector.



In March, many oil tankers carrying Russia-related cargo reflagged from Liberia and the Marshall Islands to other jurisdictions, following US pressure, and in the same month, India's Reliance Industries, one of the country's largest businesses, stopped buying oil shipped by Russia's largest shipping firm, Sovcomflot (SCF). In August, the UAE refused to accept ships flagged under the African nation of Eswatini following reports that they were being used by both Russia and Iran to enable sanctions evasion efforts.

In parallel with these efforts, Western countries also continued to try and leverage value for Ukraine from Russian state assets, frozen as a result of sanctions. According to most estimates, up to $350 billion worth of Russian state assets have been frozen since the start of the war, with most of these funds held by the European securities depository, Euroclear. During 2024, significant progress was made on this challenge, – but it remained fraught with legal difficulties. In April, President Biden signed an act that would allow the US president to seize Russian state assets in the US (worth around $5 billion) and provide them for humanitarian assistance to Ukraine. In May, the EU also agreed to a new regulation that enabled the use of net profits from Russian state assets held in the EU to support the Ukrainian war effort and reconstruction, leaving the underlying assets intact as Russian state property.

This latter initiative was expected to generate over $3 billion a year to support Ukraine. Other efforts continued to try to move from 'freeze to seize' for the sanctioned assets of oligarchs, but this has proved extremely problematic for many countries as there is typically no legal basis to seize the private assets of citizens due to their state's actions, regardless of their relationship to the regime in question. The most acceptable basis for doing so is evidence of criminal activity. However, there have been some positive developments in this area. In July, for example, the NCA seized $1.4 million in assets from the estate manager of sanctioned Russian oligarch Petr Aven after convincing a court that the manager had moved the funds illegally to avoid UK sanctions.

Several other sanctioned oligarchs also struggled with courts over restrictive measures, failing to have them removed after long legal wrangles. At the end of 2023, Roman Abramovich failed to overturn EU sanctions against him, and in February 2024, the European Court of Justice (ECJ) rejected similar appeals for removal from Uzbek oligarch Alisher Usmanov and Russia's first deputy prime minister, Igor Shuvalov. Also in February, Eugene Shvidler, an associate of Abramovich's, lost an appeal in a UK court against the previous decision to uphold his designation under the UK sanctions regime.

Further Russia sanctions

Other illicit activities involving Russian entities and nationals – not always explicitly related to the war in Ukraine – were also targeted by the US and its allies in 2024. An important focus of activity was the Russian Private Military Company (PMC), formerly known as the Wagner Group. Despite the demise of its founder, Yevgeny Prigozhin, in August 2023, the group continued to operate as a Russian expeditionary force in the developing world, especially Africa. These African activities were the primary target of Western measures in 2024, especially the group's involvement in illicit logging and mining in the Central African Republic (CAR), for which the US applied designations to Wagner-linked entities located in both Russia and CAR in March and May. The UK also made several designations of Wagner commanders, units, and businesses on grounds of human rights abuses, corruption, and the exploitation of natural commodities in CAR, Mali, Sudan, and Libya. These included the November designations of the 'Africa Corps,' Wagner's new operating name in Africa, and the group's commander in Libya, Andrey Averyanov.

Another important category of target for restrictive measures was Russian state-linked covert activity, chiefly in the realm of offensive cyber operations. Disentangling state from non-state actions in the cyber realm can often be difficult, but OFAC took several actions against Russian cyber attackers that were clearly badged as state-linked. This included the listing in June of twelve figures in the senior leadership of Russian technology firm AO Kaspersky Lab over its alleged cooperation with Russian intelligence. The company and another within the Kaspersky group were also added to the BIS Entity List, making it impossible to sell the company's anti-virus software in the US. In July, OFAC also sanctioned two hackers from the Russian group, the Cyber Army of Russia Reborn (CARR), an ostensibly 'independent' hacktivist group that has mounted cyber-attacks on US critical national infrastructure (CNI), Ukraine, and government departments and businesses in countries that have supported Ukraine. The EU also targeted state-linked Russian cyber actors in June, sanctioning two members of the Callisto Group and two members of the Armageddon Hacker Group, both linked to Russian intelligence, which used phishing attacks and malware to steal data from and disrupt the operations of EU governments.

Further areas of Russian illicit covert activity were targeted, too, including OFAC's September designations of Russian officials, media executives, and business fronts for efforts to interfere in the US 2024 presidential election. According to OFAC, the initiative was led by senior figures at Russia Today (RT), Russia's major overseas-focused broadcaster, and techniques such as generative AI, deepfakes, and information operations were used. In October, the EU introduced a new sanctions framework intended to target Russian hybrid warfare techniques such as sabotage, subversion, and the weaponization of illegal migration. In the same month, the UK also targeted Russia's battlefield use of chemical weapons in Ukraine and their past use against civilians in the UK in 2018, designating a variety of senior officers, units, and labs in the Russian armed forces involved in Russia's chemical weapons program. In November, the UK also designated Denis Sergeev, a Russian military intelligence officer who allegedly provided direct support for the attempted poisoning of Sergei Skripal.

Finally, Western states were active in applying their human rights sanctions regimes against alleged abuses within Russia.

The mistreatment and death of leading Russian dissident Alexei Navalny in February led the US, the EU, and the UK to make a number of targeted designations, including several Russian penal officials and two Arctic penal colonies in which Navalny was held before his death. In January, the EU imposed measures against members of the Russian judiciary involved in human rights abuses, including those against Russian dissident Vladimir Kara-Murza and the state-linked Safe Internet League, a group that targets online dissent on the Kremlin's behalf. The EU also designated the League's director, Ekaterina Mizulina. The EU added further Russia-related human rights designations in July, which included Evgeniy Sobolev, the chief prisons official in occupied Kherson in Ukraine. According to the EU, Sobolev led a prison system that used systematic torture, excessive punishments, and sexual and gender-based violence.

Evasion finds a way

However, despite their volume and range, Western sanctions have faced obstacles in their implementation. Although Western courts have sometimes found against sanctioned oligarchs, designated Russian individuals have had successes, too. In April, the ECJ found in favor of oligarchs Petr Aven and Mikhail Fridman, deciding there was not enough evidence to support their role in the Russian attack on Ukraine.

A report published in May 2024 by the Royal United Services Institute (RUSI), a think tank, highlighted how professional 'enablers' in the legal, financial, and professional services sectors – parts of which it has called "the wealth defense industry" – were continuing to work on behalf of Russian figures, often through oligarchs' associates, family members, and intermediaries.

Outside of the courts, oligarchs have also continued to find ways to evade restrictions. In January, the NCA issued an alert suggesting that high-net-worth individuals, including Russian oligarchs, were holding value in works of art held in specialist storage facilities as a way to avoid having their assets frozen. Oligarch workarounds through third countries continued to emerge, too, with certain neutral jurisdictions becoming the primary home for Russian money. In May, a report issued by the EU Tax Observatory and Norway's Centre for Tax Research revealed that since the start of the full-scale invasion of Ukraine, Russian nationals had purchased $6.3 billion in existing and under-development property in Dubai in the UAE. This was a ten-fold increase in the levels of investment prior to the Russian invasion.

The oligarchs have not been alone in finding various ways to skirt Western sanctions, as is obvious from the previously discussed 'whack-a-mole' designations of new companies and individuals involved in trading in sanctioned exports from Russia. The Russian state and closely allied hydrocarbon businesses have continued to find a ready market for oil, both through sales within the bounds and the price cap and more surreptitiously above it. Many such 'shadow sales' have continued, with newly formed intermediary firms in jurisdictions such as UAE, Hong Kong, and Malaysia serving as cut-outs between Russia and their final customers.

Much of this oil has been going to India, Türkiye, and, above all, China. Based on figures from Chinese customs data reported in January 2024, Russia became China's primary oil supplier in 2023, jumping over other major suppliers such as Saudi Arabia. According to the figures, Russia supplied China with over 107 million metric tons of crude oil, an all-time record. Taking shadow sales into account, this figure was likely to be much higher still. Nonetheless, as the Centre for Research on Energy and Clean Air (CREA) think tank indicated in February, substantial amounts of Russian oil were also ending up on the Western market after being refined in neutral jurisdictions such as India. According to a report in May from media outlet Sky News, imports of oil refined in India into the UK had risen by an astonishing 176 percent from February 2022.

Similar patterns of booming third-country trade could also be observed in the export of other Russian commodities. Huge amounts of Russian gold have been exported to Türkiye and the UAE, helping the UAE overtake the UK as the world's second-largest hub for gold trading in 2023. There have also been indications that third-country hubs have been used to sell sanctioned items to Western countries 'by the back door.' Reporting in the spring of 2024 suggested that over 261 tonnes of Russian timber had been imported into Belgium via circuitous transshipment routes and intermediary companies in Türkiye, Bulgaria, Kazakhstan, and China. Turkish timber imports into Belgium alone showed a sixfold increase between 2021 and early 2024, which was hard to explain through a sudden rise in Turkish loggers' productivity.

Russia has also been able to continue sourcing the arms, equipment, and technology to support its war effort through the open and active support of North Korea and Iran and through the more covert activities of companies in China and other formally neutral states.

Moreover, Russia has been able to get access to items produced in sanctioning countries, too, using adapted supply chains that pass through third countries. According to an estimate provided in January 2024 by the Kyiv Institute of Economics (KSE), a research institute, and the Yermak-McFaul Working Group on Russian Sanctions, just under half of all Russia's war-related imports in the first ten months of 2023 had come from businesses operating in countries which had imposed sanctions on those items. Further reporting throughout the year provided further evidence; in May, the Lithuanian media outlet LRT reported that at least 130 million euros of dual-use goods (equivalent to around $137 billion) had been shipped from Lithuania to Russia, chiefly via Central Asian countries.

Western-made consumer goods have also made their way to Russia via similar routes despite restrictions. Car imports into Russia from Caucasian countries such as Georgia and Azerbaijan have shot up since the war began in 2022. According to Sky News, while UK car exports to Russia ceased in 2022, its exports to countries in Russia's orbit, especially Azerbaijan, ballooned in size. The analysis noted that UK-Azerbaijan trade figures for 2023 indicated a

1,860 percent increase in UK car exports to Azerbaijan compared to the five years prior to the invasion.

And while much of the effort to source military, dual-use, and consumer goods appeared to have been coordinated by intermediaries based in neutral jurisdictions, Western countries were also vulnerable to direct exploitation. In January, the Dutch authorities seized the assets of a group of Netherlands-centred businesses that were being used to sell electric, technical, and laboratory equipment to Russia. The following month, media reports alleged that a former member of the GRU, Russia's military intelligence agency, had been using an office in Brussels to source and supply high-tech machine tools made in European countries and supplying them to Russia via Türkiye to support the production of hypersonic missiles. Western governments were right to target the lax attitude of third countries, but they needed to look closer to home, too.

Belarus and sanctions evasion

The Putin regime has been the main target of Western sanctions activity with regard to the war in Ukraine; however, it should not be forgotten that Russia's neighbor and non-combatant ally, Belarus, has also been heavily designated in its own right, both for its support for Russia's war, and its repressive behaviors at home. Many of the restrictive measures against Belarus by the US, EU, and UK have mirrored those taken against Russia, although they have tended not to be as extensive or wide-ranging. As a consequence, Belarus has become one of Russia's **partners of choice** for sanctions evasion efforts. In response, Western states sought in 2024 to close off options for Russia to use Belarus as a conduit towards the outside world. In April, OFAC targeted Belarusian state-owned enterprises (SOEs) and individuals linked to the Lukashenko regime for involvement in an **arms procurement scheme**, and in August, designated 14 individuals 14 entities involved in **military procurement and the transshipment of sanctioned goods** to Russia and an aircraft used personally by Lukashenko. In June, the **EU also tightened its measures against Belarus**, implementing new sanctions on the export of dual-use goods and technology to Belarus and the import of Belarusian metals and minerals. It also banned commercial transport with Belarus by road and required its exporters to insert a 'no-Belarus clause' in all future commercial contracts. In addition to Belarus's role in sanctions evasion, the **EU** and **Canada** also imposed further sanctions on several individuals involved in ongoing human rights abuses in Belarus in government departments, the judiciary, and the penal system.

No magic bullet

The main aim of Western sanctions against Russia has been to coerce the Putin regime into ending the war against Ukraine by undermining its capacity to prosecute its military campaign, weakening the Russian economy, and degrading the resolve of the political, military, and business elites on whose support Putin depends. After nearly three years of progressively tightening Western sanctions, they have so far failed to achieve their aims. The Russian war effort continues to advance slowly, Russian military production continues to grow, and the Russian economy continues to outpace its Western opponents. According to figures from the IMF issued in April, the Russian economy was predicted to grow faster than all the advanced economies in 2024. Some Western economic observers have suggested that the Russian economy will collapse eventually, overheated by onerous demands and starved of necessary products, but it is not clear that this will happen soon.

There are several reasons why sanctions have had a limited impact. Firstly, the Russian economy has been relatively well managed since the war began, overseen primarily by Elvira Nabiullina, Head of Russia's Central Bank. Domestic production of consumer and military items has also ramped up considerably. Furthermore, the Russian authorities have been willing to innovate when it comes to trade, encouraging the use of third-country workarounds and novel payment methods such as cryptocurrencies. As Nabiullina remarked at a conference in July, Russian businesses needed to find "multiple choice solutions," also saying that "new financial technology creates opportunities for schemes which did not exist before. This is why we softened our stance on the use of cryptocurrencies in international payments, allowing the use of digital assets in such payments".

But while Russia has proved resourceful, it has also been aided and abetted by third countries and the West's unforced errors. Many sanctions have been announced but not immediately imposed. Although this has been intended to allow Western companies time to retrench and adapt, it has also allowed Russian sanctions evaders to find alternative methods to continue trading. Sanctions have also been partial in scope, leaving many crucial gaps and exceptions that have been open to exploitation. For example, there are no restrictive measures against refined oil from non-Russian refineries, providing an easy route for Russian oil to come back to markets from which it has theoretically been banned.

At the same time, Western governments' enforcement of sanctions has been relatively weak, even amongst those that have been at the forefront of taking action with new designations. In a report from July 2024, Spotlight on Corruption, an advocacy group, noted that despite the UK's readiness to apply sanctions against Russia, there had been no fines, convictions, or seizures related to those sanctions up until that point. The UK's sanctions effort, it stated, was "all bark and no bite." Evidence from the end of the year suggested that the UK was beginning to pivot towards tougher action, with the UK's Financial Conduct Authority (FCA) and Office of Financial Sanctions Implementation (OFSI) taking a harder line on breaches in the autumn. However, only two actions were taken, and in the case of the OFSI enforcement, the fine was incredibly small (equivalent to just over $19,000). The UK was beginning to bite, but by year's end, its teeth marks remained fairly superficial.

Russian sanctions on the West

While the weight of sanctions activity has been directed by Western countries against Russia, Russia took retaliatory action in the early days of the war, including a range of "**special economic measures**" to reduce Western access to Russian financial markets. Russia has also extended its **food import ban** against US, EU, and Australian produce, which began in 2014. The Russian Ministry of Foreign Affairs has also imposed various personal financial sanctions and travel bans against officials, politicians, businesspeople, academics, and media figures in various Western countries for holding "anti-Russian views." In 2024, among the new designations were 18 individuals in the **UK**, listed in February, and 140 individuals in **Australia and New Zealand**, listed in October.

Prospects for 2025

It is highly likely that with the return of President Trump, the US will exert greater pressure on Ukraine to come to terms with Russia, quite possibly involving the loss of some of its territory. Whether Ukraine will be willing to accept this is another matter, although its precarious position on the battlefield and dependency on Western support – and especially US support – will force it to agree to negotiations, if not yet a settlement. Russia is also likely to be willing to negotiate, encouraged by China, especially when it reaches what it assesses to be the high watermark of its advance in the east and south. However, while the Russian economy remains strong, reinforcements come from North Korea, and territorial advances continue, the Putin regime's seriousness about reaching a settlement will remain doubtful. Indeed, Russia seems unwilling to countenance any compromises that Ukraine sees as essential to a durable peace, including Western security guarantees or qualified membership of NATO.

If the war continues, potentially interspersed with negotiations, how will the combatants fare on the battlefield? Both sides face serious manpower and equipment issues, but Ukraine is in a weaker position. Russia is a larger and wealthier country, and over time, the differential between its economic and military strength and Ukraine's will tell. Despite Ukrainian tenacity and determination, the Russians seem likely to continue advancing gradually throughout the year while launching successive drone and missile strikes on Ukraine's CNI and civilian population. These will not break Ukraine, but they will further wear down morale and may feed into an eventual desire to make concessions that the country is currently unwilling to consider.

It is also probable that President Putin and members of his regime will continue to make verbal threats of tactical nuclear weapons usage. However, hybrid warfare in Europe is likelier than nuclear strikes, with a rising number of acts of sabotage, subversion, provocation, and intimidation by Russian agents and proxies in Europe. These will probably become more violent and more dangerous and might even lead to a substantial loss of life. An alleged Russian plot to cause fires on cargo planes flying from Europe to the US revealed in October, is probably a taste of things to come in 2025.

The Western approach to the conflict, framed around the ongoing use of sanctions, will probably see more continuity than change, at least initially. Despite Trump's promises to end the war quickly, he will find it difficult to get the deal he wants from Putin, much as he found in his negotiations with Kim Jong-Un in his first term. Sanctions will continue, and new rounds will come from the EU, UK, and possibly more sluggish than in the recent past, the US. If Russia does prove recalcitrant, Trump might seek to increase pressure on Putin with more sanctions, threats to seize Russian assets, and tougher enforcement measures on sanctions breaches. While Trump is believed to dislike the use of military force, he remains a great admirer of the power of economic weapons.

What does this mean for me?

- With the war in Ukraine probably continuing in 2025, sanctions will remain in place for the foreseeable future. Negotiations are unlikely to lead to significant early sanctions relief for Russia, so your firm will need to ensure it maintains appropriately calibrated sanctions monitoring tools backed by a rich body of risk data. New sanctions rounds will continue, with more secondary sanctions on entities and individuals in neutral third countries. You will need agile platforms that will react quickly to changing events.
- Western governments and regulators have been stung and embarrassed by media and civil society criticisms of sanctions enforcement against Russia and will seek to change the narrative in 2025. There will be great pressure on Western authorities to show that, even if the war continues, sanctions 'work.' The easiest way for them to do that will be to take enforcement action against egregious failings in the private sector. This means you will need to review your risk management frameworks and controls to ensure they are fit for purpose.
- As long as the war continues, moreover, Russia will continue to seek ways to work around and evade sanctions, using third countries and FinTech. If you work in the payment services or crypto-asset service sectors, you should pay special attention to the risks that you face.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

The Middle East

At some points in 2024, the Middle East seemed on the path towards full-scale regional war, with Israel, Hamas, Hezbollah, and the groups' sponsors in Iran conducting a range of military and unconventional attacks against each other throughout the year. Although these conflicts are intimately connected, for ease of reference, we here divide the overall situation into two theatres, one a regional conflict between Israel and its allies against Iranian-backed Islamist terrorists and militias across the region, known as the 'Axis of Resistance' (see map), and the other, extra-regional conflict between Iran and Western states, which oppose Iran's potential pursuit of a nuclear weapon and the regime's growing ties with Russia and China.

2024

Israel versus the Axis

The year began amid ongoing Israeli military action in Gaza in response to Hamas's massacre and hostage-taking spree in southern Israel on October 7, 2023. Israel's military action in Gaza continued throughout the year. Some Israeli goals were achieved, with Hamas's military capabilities greatly impaired and the group's leader, Yahya Sinwar, killed in October. However, Hamas – as much an idea as an organization – was not annihilated. Fighting continued, and out of 251 hostages taken by the group in 2023, around 100 remained unaccounted for by year-end. Negotiations for a ceasefire and return of the hostages, hosted by Qatar, failed to come to a resolution, with Qatar suspending its role as mediator in November, despite US pressure.

Despite ongoing support for the Israeli Defense Forces (IDF) amongst the Israeli population, moreover, the country's government, a shaky national unity coalition led by Prime Minister Benjamin Netanyahu, was widely criticized for failing to get the hostages back. Netanyahu himself remained deeply unpopular, and subject to an ongoing corruption trial. There were large protests against his leadership throughout the year, including a wave in November after his dismissal of Defense Minister Yoav Gallant.

Disquiet within Israel also matched concern among the international community. The Hamas attack in 2023 had garnered widespread solidarity with Israel, but as the war continued, many countries, including Israel's friends, criticized its conduct of the war. Particular concern was expressed about the inhumane treatment of civilians – many of whom were left without food, sanitation, or basic services – as well as the efforts of Israeli settler communities to take advantage of the Palestinians' displacement in the wake of Israeli military action. Nonetheless, most Western countries kept their criticism rhetorical, and despite some token efforts to constrain military supplies for use in Gaza – the UK tightened export controls in September, for example – arms supplies coming from the US, Germany, and Italy continued.

Elsewhere, however, some countries sought to take a stronger line. Across the year, a growing number of states, both Western (e.g. Belgium and Ireland) and non-Western (e.g Cuba and Nicaragua), expressed their support for an ongoing case brought to the International Court of Justice (ICJ) by South Africa, accusing Israel of genocide in the occupied Palestinian territories. Separately, in July, the ICJ issued a finding criticizing Israel's conduct in the occupied territories, demanding its withdrawal of all military forces and civilian settlers. Israel's international legal woes were further added to in November when the International Criminal Court (ICC) issued warrants for the arrest of Netanyahu and Gallant for alleged war crimes, alongside a warrant for the arrest of Hamas military commander Mohammed Deif. Although some Western governments said they would execute the warrants if required, both the US and Israel rejected their validity, with Netanyahu describing them as "antisemitic."

Alongside its conflict with Hamas, Israel took sustained covert and overt military action against other Islamist groups and militias supported by Iran. Primary among its targets was Lebanese Hezbollah, a group with which Israel has fought periodically since the group's creation in 1982. In September, Israel surprised the group with the remote detonation of thousands of its pagers and walkie-talkies, which killed over 40 and injured over 3000. This was followed by air strikes against the group's assets across Lebanon and the assassination of the group's leader, Hassan Nasrallah, by airstrike on September 27.

At the end of that month, the IDF launched a ground offensive against the group in southern Lebanon, with further airstrikes targeting the group's military and political leadership. On November 27, after sustained pressure from the US and other states, a ceasefire came into effect. However, despite President Biden hailing a "permanent cessation of hostilities," both sides had continued attacks against the other right up until the deadline, and with Israeli forces remaining in southern Lebanon, peace seemed fragile at best.

Israel also launched a major 'one-off' set of air strikes against the Houthis in Yemen in July 2024; the group had been firing missiles at Israel and interfering with Western shipping in the Red Sea in self-described solidarity with Hamas. Israel showed more forbearance toward the Iranian-backed Shi'ite militias of Iraq, which increased drone and missile attacks against the Jewish state throughout the autumn of 2024, but most observers expected an eventual Israeli military response.

Interweaved with these individual conflicts between Israel and different terrorist groups and militias was Israel's ongoing confrontation with the groups' main state backer, Iran. Historically, the regimes in Tehran and Israel had tended to avoid direct country-to-country military engagements and an escalatory cycle that might lead to war. However, in 2024 this taboo was well and truly broken. In April, following an Israeli airstrike on an Iranian consulate in Syria, which killed several leaders of the Iranian Revolutionary Guard Corps (IRGC), Iran launched 300 missiles and drones at Israel. Most of these were shot down, with additional support from Western allies and neighboring Arab kingdoms. Israel responded later in April with a precision strike on an air defense system unit in Isfahan, Iran. In July, Israel launched a further airstrike on Tehran, targeting and killing Hamas's political chief, Ismail Haniyeh, who was visiting Iran for the inauguration of the country's new president. Iran made no immediate response, but in early October, fired up to 200 missiles at Israel, describing the strikes as retaliation for the assassination of various Hamas, Hezbollah, and IRGC leaders. Israel returned fire later in the month, targeting Iranian air defenses and military targets but not the nuclear facilities or oil logistical hubs that some Western hawks had wanted.

In November, Iran's Supreme Leader, Ayatollah Khamenei, vowed "a teeth-breaking response" to the Israeli attacks, sustaining a pattern of tit-for-tat that showed no likelihood of stopping in the immediate future.

Funding the Axis

In parallel with the military struggle, 2024 was a financial battle against Iran's Axis of Resistance, involving not just Israel, but the US and its allies too. According to a detailed advisory from FinCEN, issued in May, all of Iran's proxies have two main categories of funding – self-generated financing, and state-based support from Iran.

In the first case, Hamas has relied upon tax-based and commercial income from its control of the Gaza Strip – mostly now gone – as well as income from a global investment portfolio, 'charitable' donations, and online crowdfunding through social media and instant messaging platforms. Crowdfunding donations have come in both fiat and cryptocurrency, channeled through accounts and wallets in third countries such as Qatar or Türkiye. Hezbollah, by contrast, has enjoyed more extensive financial interests, including a wide global network of interconnected businesses and investments. Some of its activities are apparently legitimate, while others, such as narcotics smuggling and illegal mining, are plainly not. Hezbollah's network commonly uses front companies, often described as nebulous 'import-export' businesses, as well as religious charities or educational institutions to operate. In these endeavors, Hezbollah works in collaboration with sympathetic governments, such as Syria and Venezuela, OCGs, such as various Latin American cartels, and other terrorist organizations, regardless of ideology, including the Marxist-Leninist FARC group in Colombia. Other members of the Axis – the Houthis, the Iraqi militias, and the smaller Gaza-based Islamist group Palestinian Islamic Jihad (PIJ) – are less well-placed financially but have managed to generate funds through an assortment of means, including the collection of taxes or customs due in areas they occupy (alternatively described as extortion), illegal appropriation of public and private assets, criminal activities such as counterfeiting, and donations.

The second source of financial support for the groups is, of course, Iran. According to US government estimates, around $700 million of Hezbollah's annual budget of $1 billion comes from Iran, while Hamas has received as much as $100 million a year since 2018. Iran largely generates these funds through its 'shadow economy' (see box), where the profits of illicit oil sales are used to fund the purchase of sanctioned goods for Iran, as well as the overseas activities of the IRGC and Iran's proxies. Historically, these funds have been channeled from Iran to the groups through various channels, such as cash and gold smuggling, fake remittances, TBML techniques, international payments via front companies, exchange houses, and sham charities. However, the IRGC has increasingly sought to involve its proxies directly in the management of oil sales, allowing them to take their cut and manage the disbursement of funds. Hezbollah has played a particularly significant role here, as has Iran-based Houthi facilitator Sa'id al-Jamal, who has become a central figure in managing Iran's financial relationship with the Axis of Resistance.

Iran's shadow economy

Iran's shadow economy is driven by the sale of illicit oil and oil-related products. According to the **US Congressional Service**, nearly all current Iranian oil exports go to China. These exports are sold through a complex web of front companies based in third countries such as UAE and transported via a 'shadow fleet' of tankers that operate without transponders to avoid detection and use false documentation, circuitous routes, and ship-to-ship transfers to obfuscate their origins. Their deliveries usually go to independent rather than state-owned refineries in China, known as 'teapots,' which then rebadge the origin of the oil as Iraqi, Omani, or Malaysian.

The Atlantic Council, a think tank, notes that many of these teapots will only pay for Iranian oil in Chinese renminbi, which has limited convertibility, meaning that Iran has to use these funds to buy Chinese goods (machinery and electronics are preferred purchases, or leave the funds in China as overseas reserves. However, as a separate investigation by **The Economist** has suggested, Iran has also been able to source US dollars and euros through sales to China and elsewhere, using exchange houses and small banks to move funds internationally through correspondent accounts. These funds are then used by front companies to buy sanctioned goods, services, and commodities.

The financial battlefield

Israel has sought to undermine its opponents' financial infrastructure with kinetic actions, including airstrikes on the branches and vaults of the Hezbollah-linked Al-Qard Al-Hassan Association (AQAH), a not-for-profit financial association in Lebanon. Less dramatically, Israel has also applied financial sanctions to 24 clients of AQAH that it alleges support Hezbollah operations. And while not participating in Israel's offensive military actions, its Western friends and allies have sought to provide substantial support on the financial battlefield instead, applying their own extensive financial measures against Iran's proxies.

In 2023, in the wake of the October 7 attack, the US implemented a raft of designations against networks of Hamas financial facilitators and institutions located in Gaza and across the Middle East, including cryptocurrency and money transfer business Buy Cash. The US and UK also took co-ordinated action against senior officials of Hamas and Palestinian Islamic Jihad (PIJ), another smaller Gaza-based Islamist group aligned with Iran, in November and December 2023. Further designations by the US and its allies followed throughout 2024:

- **In January,** the US, UK, and Australia took joint action against Hamas, PIJ, and IRGC financial facilitators, including the front businesses and financial institutions of the Shamlakh and Hirzallah families. The European Union also created a "dedicated framework" of sanctions focused on Hamas and PIJ, designating Yahya Sinwar and several Hamas financial facilitators, including the Sudan-based Abdelbasit Hamza Elhassan Mohamed Khair.

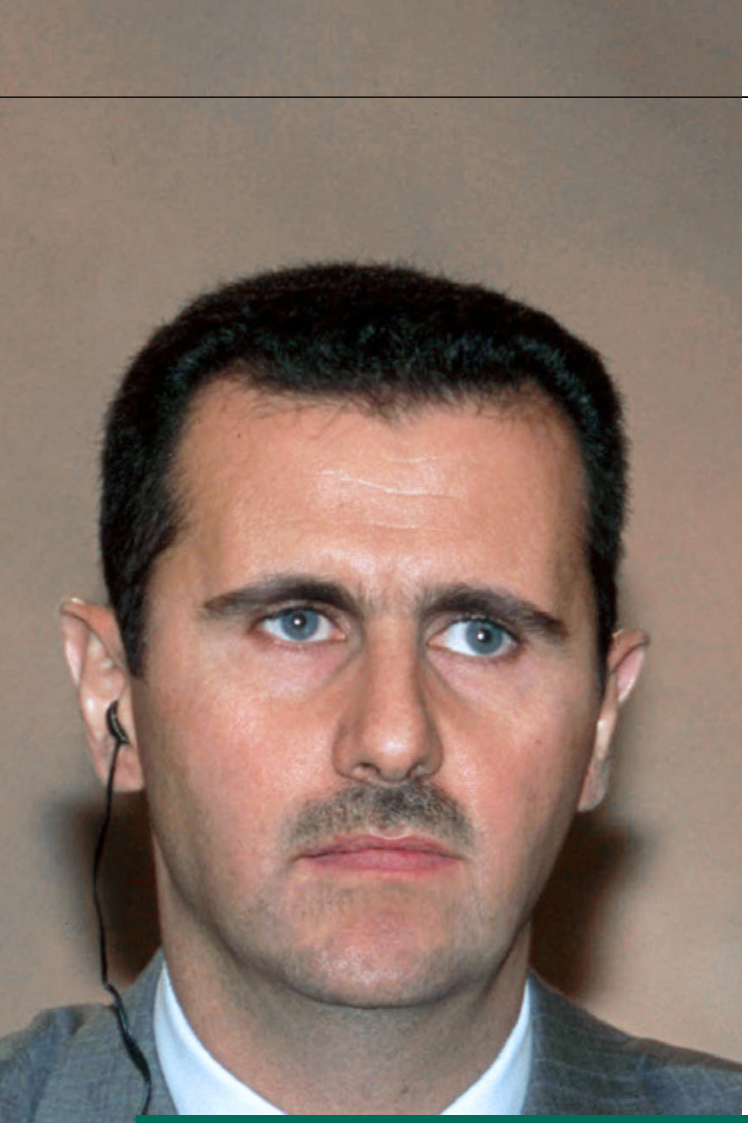
- **In March,** the US and UK announced action against the fundraising body Gaza Now and linked entities and individuals.
- **In April,** the US targeted senior Hamas drone and cyber unit commanders, while the EU issued concurrent sanctions related to Hamas's alleged use of sexual and gender-based violence.
- **In June,** the EU listed Hamas and PIJ fronts, including several controlled by Sudan-based financier Khair and several other facilitators, including Zuhair Shamlakh of the Shamlakh network.
- **In October,** the US designated Hamid Al Ahmar, a Türkiye-based Yemeni businessman and Hamas fundraiser, several Europe-based Hamas financial facilitators, a sham charity, and the Hamas-linked Al-Intaj bank.
- **In November,** the US designated six Hamas officials and financial facilitators operating in Gaza and Türkiye, who helped funnel funds into Gaza from other countries, including Russia.

Beyond Hamas, the US added further designations intended to target Iran's shadow economy and the flow of funds to proxy groups arising from it. Hezbollah was a major target, with fresh designations of Hezbollah-linked fronts, vessels, and financial facilitators coming in January, March, August, and mid- and late September. One scheme involved the sale of Iranian LPG to the Assad regime, from which Hezbollah facilitators Muhammad Qasir and Muhammad Qasim al-Bazzal funneled funds to the group. The US also designated the Hezbollah-linked money laundering network of Hassan Moukalled, based in Lebanon and UAE, in May, and other members of the Hezbollah financial network in October. Other Western countries took less extensive or intensive financial and economic action against Hezbollah, with both the EU and the UK preferring to encourage ceasefire discussions over the application of new punitive measures. However, the UK did impose a travel ban on Nazem Ahmed, a previously sanctioned Lebanese businessman and alleged Hezbollah financier, in August.

Besides Hezbollah, the most intense range of designatory actions was directed at the Houthis, both for their military actions in the Red Sea and for their involvement in the illicit Iranian oil trade.

Here, there was considerable coordination between the US and the UK throughout 2024:

- **In January,** OFAC designated companies in Hong Kong and UAE that allegedly sold and shipped Iranian commodities on behalf of Houthi facilitator Sa'id al-Jamal, as well as blocking four vessels involved in the trade. In joint action with the UK, OFAC also designated several senior Houthi officials, including Mohamed al-Atifi, the Houthi Defense Minister, and Muhammad Fadl Abd al-Nabi, the commander of Houthi naval forces.
- **In February,** the US and UK jointly designated Mohammad Reza Fallahzadeh, the IRGC commander supporting Houthi operations. The UK designated Sa'id al-Jamal, a senior Houthi official, and several units of the IRGC that support Houthi activities.
- **In March,** OFAC issued three packages of designations (March 6, March 15, March 26) on shipping companies based in Hong Kong, the Marshall Islands, Liberia, India, and Vietnam, used by Sa'id al-Jamal to transport oil to China, as well as various associated vessels flying under flags of convenience.
- **In June,** OFAC designated Ali Abd-al-Wahhab Muhammad al-Wazir, a China-based Houthi facilitator and associated entities, for enabling Houthi weapons procurement, especially parts for drones and missiles. Further individuals, businesses, and vessels involved in the al-Jamal network were listed.
- **In July,** OFAC designated several more individuals, entities and vessels associated with the al-Jamal network, including Indonesia-based Malaysian and Singaporean national Mohammad Roslan Bin Ahmad, and China-based Chinese national Zhuang Liang. In a separate designation, OFAC targeted various Yemen, Hong Kong and China-based businesses and associated shipping firms involved in procuring banned military items from China.
- **In August,** OFAC added further designations of individuals, businesses, and ships linked to the al-Jamal network of illicit oil and LPG sales to China.
- **In October,** OFAC designated further companies and individuals involved in Houthi drone and missile parts procurement in China and further elements in the al-Jamal network.



- **In November,** OFAC also sanctioned numerous companies, individuals, and vessels associated with the major Syrian corporate group, the Al-Qatirji Company, which helped generate funds for the IRGC and the Houthis by facilitating Iranian oil sales to Syria and China. The group had previously been designated by the US for its role in facilitating oil sales between ISIS and the Assad regime.

The US also took action against several smaller Iranian proxy groups, designating leaders of the Iraqi militia Kata'ib Hizballah in January, along with a linked front company and business associate, and operatives of the Al-Ashtar Brigades in March, an Iran-based Shia militia group hostile to the authorities in its native Bahrain. In a major action against the broader financial framework of proxy funding in the region, FinCEN issued a final rule under the Patriot Act in June, declaring Al-Huda Bank, an Iraqi bank, as a conduit for terrorist financing and being of "primary money laundering concern," barring US financial institutions from engagement with it; its owner and controller, Hamad al-Moussawi, was designated in January.

Syria, Iran's difficult friend

Since March 2011, Syria has been subjected to a vicious civil war between the Iranian-backed regime of Basher al-Assad, Hezbollah, Islamist groups including ISIS, and others linked to Al Qaeda, secular groups backed by the West, and Kurdish fighters. Russia, Türkiye, Israel, and the US have also intervened from the outside to varying degrees. In recent years, the Assad regime had increased its territorial control across Syria with Russian support, but the dramatic collapse of its forces at the end of 2024 led to the end of the Assad era and the appointment of **Mohammed al Bashir** as head of a transitional government. Bashir had previously overseen areas of Syria under rebel control. With the transitional government intending to stay in power through March 2025 "until the constitutional issues are resolved," the medium-term future for Syria remains deeply uncertain.

The Assad regime was targeted with sanctions by the **US** for over four decades, largely related to the regime's support for international terrorism.

With the start of the civil war in 2011, the US implemented further packages of sanctions against the regime for its repression of the Syrian people, including the **Caesar Syria Civilian Protection Act** 2019, which designated Assad and his regime for war crimes. The **EU**, **UK**, and others also imposed sanctions on the regime for its human rights abuses, war crimes, and criminal activities. In 2024, Western states continued to impose new restrictions. The regime's involvement in the illegal drugs trade, especially the synthetic drug Captagon, led to OFAC designations against traffickers, front companies, and enabling Syrian officials in **March** and **October**. The EU also targeted individuals and entities linked to the Assad family, the regime's drug trafficking, civilian repression, and human rights abuses in **January**, **July**, and **November**. Notable listings included several Syrian civilian air firms and Damascus-based Freebird Travel Agency for involvement in drug trafficking and senior Syrian soldiers Abdel Karim Mohammad Ibrahim and Ali Mahmoud Abbas for using sexual violence and torture as a weapon of war.

Targeting Israeli extremism

Besides Western actions against Islamist extremist groups, the US and its allies have also taken action against Israeli extremist settler groups that blocked humanitarian assistance to Gaza, intimidated Palestinians, and extended illegal settlements in the West Bank and East Jerusalem. In February 2024, President Biden issued an executive order providing the legal basis for the administration to impose sanctions on those threatening stability in the West Bank, which was accompanied by the designations of four settlers by the US Department of State and with further individual and entity designations by the State Department in March and July. OFAC applied sanctions to settler organizations Hilltop Youth and Amana, as well as individuals and entities involved in crowdfunding for the settlers. The EU also took action, using its Global Human Rights Sanctions Regime to enable restrictive measures against extremist settler organizations such as Lehava and Hilltop Youth and associated individuals, in April and July. The UK took similar measures in February, May and October.

Iran and the West

Iran and its allies were, however, more than just a problem for Israel or its Sunni Arab neighbors in the Persian Gulf. As noted above, Iran has long had wider aspirations on the regional and global stage, including dominating its own region, supporting the efforts of Russia and others to reshape the rules-based international order, and - potentially - developing a nuclear weapon.

The US, and to a lesser extent its allies, have sought to meet the Iranian challenge with wide-ranging sanctions targeting its ability to source and fund technology required to build weapons of mass destruction (WMD) and ballistic missiles. The most important of these have been UN, US, and EU measures against WMD proliferation, which led to UN, US, and EU sanctions on Iran's export of oil and gas. These were eased in July 2015, with the agreement of a Joint Comprehensive Plan of Action (JCPOA) between Iran and the five permanent members of the UNSC (US, China, Russia, France, and the UK), with Germany and the EU.

However, President Trump unilaterally withdrew the US from the agreement in May 2018, and in September 2023, France, Germany, and the UK announced they would retain sanctions due to be lifted because of Iranian non-compliance with the agreement.

In the first years of the Biden administration, the US sought to re-engage Iran, but despite initial progress in talks about the return of the US to the JCPOA, discussions were stymied by the summer of 2022, partly as a result of International Atomic Energy Agency (IAEA) assessments that Iran was producing highly enriched uranium, close to levels needed to make a bomb. Further major obstacles to agreement arose after Russia's full-scale invasion of Ukraine in 2022, as Iran provided the Russian army with increasingly sophisticated drone technology for use on the battlefield and beyond. Iran also began to align itself closely in both political and economic spheres with other US adversaries, especially China. The US, EU, UK, and others responded to these activities by imposing a variety of sanctions throughout 2022 and 2023 against Iranian military officers, officials, businesspeople, and public and private entities involved in providing military support to Russia. The Western allies also imposed a raft of designations following the death in police custody of Mahsa Amini on September 16, 2022, and for regime brutality against Iranian civilians protesting in its wake.

Hopes and realities

Despite the bleak backdrop of previous years and the rising tensions between Iran and Israel throughout 2024, there were some opportunities for a return to cooperation with the West. Despite an absence of active talks to return the US to the JCPOA, neither side stated that they had believed that they were over completely. Unexpected events also took a hand. In May, a helicopter crash led to the death of President Ebrahim Raisi, a hardliner, and in a two-round presidential election in June and July, the most moderate candidate, Masoud Pezeshkian, a former cardiac surgeon, was elected. While remaining loyal to the regime, Pezeshkian's campaign stated a desire for better relations with the West, a revised nuclear deal and accompanying sanctions relief, and reduced tensions with Iran's regional neighbors. The new president sought to make good on these aspirations with a speech to the UN on 25 September, pledging "a new era of cooperation."

Nonetheless, Pezeshkian's rhetoric, while welcome, did not appear to have an immediate impact either on Iran's relationship with the West or Iran's wider conduct. Indeed, his foreign minister, Abbas Araghchi, stated in August that Iran was interested in "managing hostilities" with the US, not ending them. Behind Pezeshkian, moreover, both the IRGC and Ayatollah Khamenei – the latter unarguably the most powerful decision-maker in Iranian foreign policy – continued to take a more hostile stance towards the US and its allies, and one more in line with the regime's ongoing support for the Axis of Resistance and its direct attacks on Israel.

Tightening core sanctions

Unsurprisingly, therefore, 2024 saw further Western attempts to tighten the sanctions regime against Iran's shadow trade in sanctioned oil and oil-based products, used partly to fund its proxy groups (discussed above) but also to support its own economy and weapons program. A major US target was Iran's Ministry of Defense and Armed Forces Logistics (MODAFL), which also relied on income from sanctioned oil and used the same model of intermediary sales as the IRGC. In February, April, and June, OFAC designated various aspects of MODAFL's oil-selling operations, including companies registered in Hong Kong, the Marshall Islands, the UAE, and numerous associated vessels. OFAC also continued its long-running designations of the global shadow shipping network developed by the already designated Iranian state-linked businesses, the National Iranian Oil Company (NIOC) and Triliance Petrochemical. Extensive designations of these companies' fronts and vessels were published by OFAC in October and December. Efforts against the Iranian state's logistical and commercial network were supplemented in June with designations of nearly 50 exchange houses and front companies in Hong Kong and the UAE, used to support the oil sales of both the IRGC and MODAFL.

Alongside the key target of the Iranian oil trade, the US focused on Iran's ongoing efforts to procure sanctioned items, especially advanced technology, on the international market. In February, OFAC designated individuals and entities in a procurement network based in Iran, UAE, and Türkiye, which facilitated the export of banned US computer technology for use in Iran, including by the Central Bank of Iran (CBI). In March, OFAC further designated individuals in three procurement networks, based in Iran, Türkiye, Oman, and Germany, that have sourced items for Iran's WMD and ballistic missile programs, such as carbon fiber and epoxy resins. The following month, the BIS imposed new export controls to restrict Iran's access to low-grade technology, including basic microelectronics produced by US companies that could be used in drones and other military devices.

Drone technology featured in a further area of US action – the targeting of Iranian and third-country institutions, firms, and individuals supporting the Russian war effort. Four missile and drone suppliers based in Iran and Hong Kong, involved in the manufacture of Shahed-series drones used widely by Russia in Ukraine, were designated in February. In April, OFAC targeted 16 individuals and various entities involved in Iran's drone production, including the IRGC's drone production arm, Kimia Part Sivan Company (KIPAS), and MODAFL's front company, Sahara Thunder.

Additional designations followed in May and July, linked to MODAFL's attempts to procure drone parts through individuals and companies based in Iran, Hong Kong, and China. The US further targeted the logistics behind the Iran-Russia drone trade in September, designating ten individuals and six entities in Iran and Russia for enabling the delivery of drone and ballistic missile technology. Four vessels were also designated as blocked property.

Many of these US-implemented designations were undertaken in tandem with measures by its allies in the EU, UK, Canada, and Australia.

The EU broadened the scope of its restrictive measures against Iran to include the supply of missiles and drones to Russia and imposed designations on senior Iranian officials (including both the Defense Minister and his deputy), military figures, institutions, and businesses (including several Iranian airlines and shipping firms), in tranches released across May, October, and November. The EU's November measures also included a new ban on transactions with ports and locks linked to the logistical transfer of drones, missiles, or related technologies, such as Amirabad and Anzali on the Caspian Sea. The UK also took extensive action on Iran in 2024, targeting Iranian drone production in April, including new export controls on drone parts. In alignment with the US and several European countries, the UK targeted drone production and logistical supply in September and November, including the designation of Iran's national airline, Iran Air. Australia also imposed its own sanctions on senior Iranian military figures, officials, and business figures involved in drone production in May and October.

Other sanctions on Iran

Other areas of unethical or illicit Iranian activity prompted US sanctions designations. In January, OFAC, in conjunction with UK authorities, designated individuals within an assassination network led by Iranian narcotics trafficker Naji Ibrahim Sharifi-Zindashti, linked to the Iranian Ministry of Intelligence and Security (MOIS). The network was alleged to have been behind several state-backed murders of Iranian dissidents in the UK, Canada, Türkiye, and UAE. In September, the US, in coordination with Canada and Australia, designated officials in the IRGC and Iran's Prisons Organization for involvement in repression both at home and overseas, especially against women and girls. Other designations touched upon Iran's offensive cyber operations. These included in February and April OFAC designations of commanders, operatives, and front companies associated with the IRGC's Cyber-Electronic Command (IRGC-CEC), which were alleged to have been responsible for "malicious cyber activities," including attacks on US, European and Israeli CNI. Several individuals in the IRGC and an Iranian cybersecurity firm, Emennet Pasargad, were also designated in September due to alleged Iranian efforts to interfere with the US presidential elections through 'hack and dump' operations of sensitive data during the 2020 and 2024 US presidential elections.

The impact on Iran

During 2024, several examples emerged which indicated that Western efforts to tighten the sanctions regime against Iran were having some effect. On a tactical level, several cases of evasion were identified and tackled; in February, for example, the US Department of Justice (DoJ) announced charges in separate cases of Iranian oil-related sanctions evasion. In New York, charges were laid against an IRGC officer and a Turkish energy company alleged to have trafficked Iranian oil to buyers in China, Russia, and Syria. Separately, in the District of Columbia, a Chinese national and Omani national were charged with offenses related to the trafficking and selling of Iranian oil to Chinese government-owned refineries.

On a strategic level, moreover, sanctions continued to have a dramatic effect on the Iranian economy. Despite joining the BRICS group of emerging economies in early 2024, Iran continued to face high inflation and low growth, with no immediate prospect of its economic performance improving, according to the International Monetary Fund (IMF).

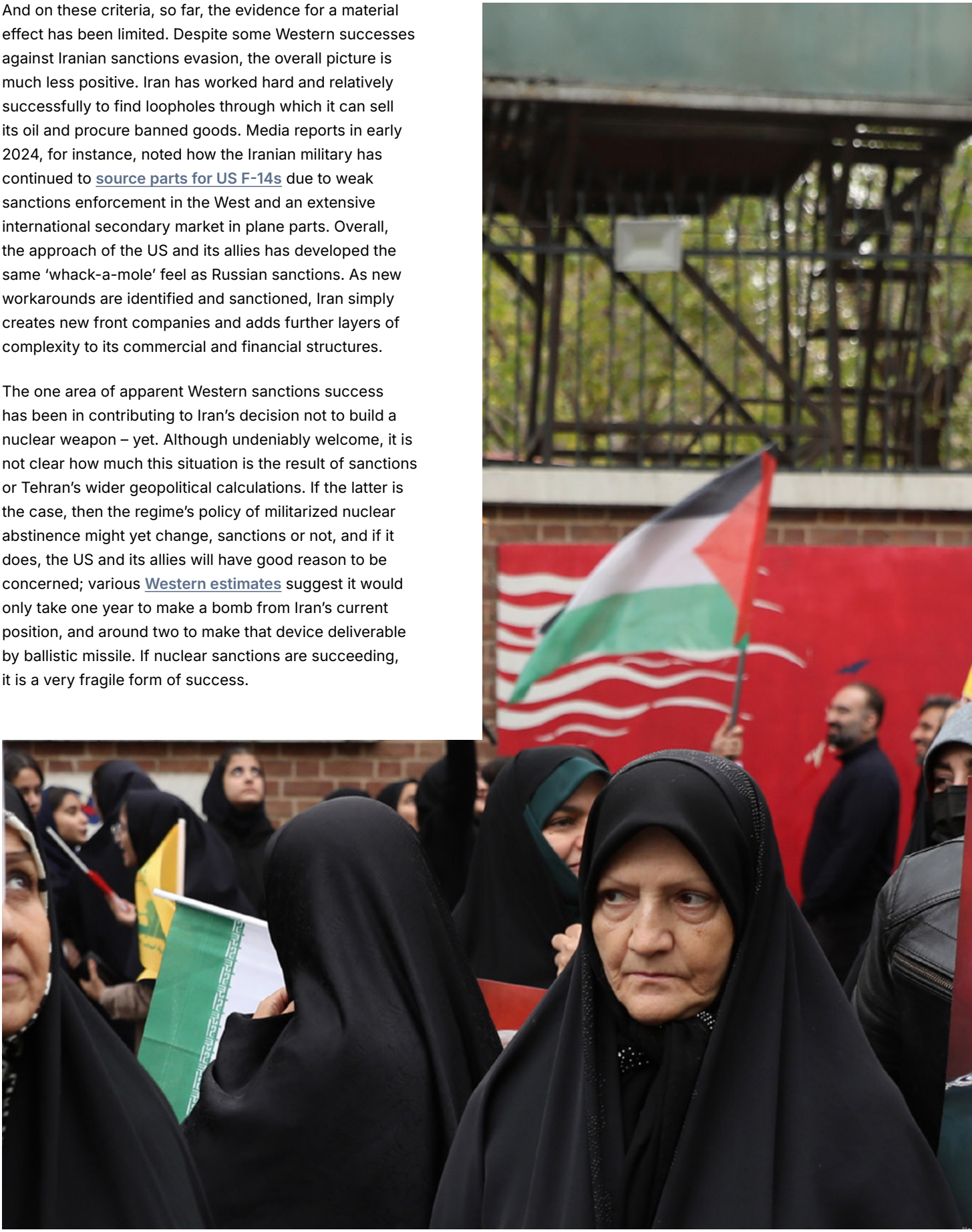
The effect of sanctions was further compounded by inefficiency, political incompetence, and corruption within Iran itself, as evidenced by the country's ongoing energy crisis.

This situation, with its various causes, also fed into wider political discontent within Iran, leading to strikes and protests over wages and the cost of living. Combined with continuing unhappiness about domestic repression of women and bold demonstrations such as the young woman who stripped to her underwear in public in Tehran in November, the atmosphere in Iran suggested a regime in crisis, unloved by its own population, tied to questionable friends, and isolated from the West.

Nonetheless, despite the bleak picture for Tehran, the aim of Western sanctions has not simply been to undermine the Iranian economy but to use resulting economic and financial pressures as a means to an end: undermining Iranian weapons proliferation and forcing changes in Iranian grand strategy.

And on these criteria, so far, the evidence for a material effect has been limited. Despite some Western successes against Iranian sanctions evasion, the overall picture is much less positive. Iran has worked hard and relatively successfully to find loopholes through which it can sell its oil and procure banned goods. Media reports in early 2024, for instance, noted how the Iranian military has continued to source parts for US F-14s due to weak sanctions enforcement in the West and an extensive international secondary market in plane parts. Overall, the approach of the US and its allies has developed the same 'whack-a-mole' feel as Russian sanctions. As new workarounds are identified and sanctioned, Iran simply creates new front companies and adds further layers of complexity to its commercial and financial structures.

The one area of apparent Western sanctions success has been in contributing to Iran's decision not to build a nuclear weapon – yet. Although undeniably welcome, it is not clear how much this situation is the result of sanctions or Tehran's wider geopolitical calculations. If the latter is the case, then the regime's policy of militarized nuclear abstinence might yet change, sanctions or not, and if it does, the US and its allies will have good reason to be concerned; various Western estimates suggest it would only take one year to make a bomb from Iran's current position, and around two to make that device deliverable by ballistic missile. If nuclear sanctions are succeeding, it is a very fragile form of success.



Prospects for 2025

The Israel-Hezbollah ceasefire achieved in November 2024 raised hopes that a similar deal could be achieved between Israel and Hamas. But can such ceasefires hold? There are good reasons for both sides to halt their current military engagement; the Islamist groups have suffered massive operational damage and need time to recover, and the fall of the Assad regime suggests a regional balance of power tipping in Israel's favor. But the Israeli population – generally unhappy with the performance of Prime Minister Netanyahu – is also suffering war fatigue and the economic consequences of prolonged fighting.

Yet the thought that Middle Eastern ceasefires might yet turn into more permanent peace seems naïve, given the history of intermittent warfare between Israel and its opponents in Gaza and Lebanon. Indeed, numerous events could yet destabilize the situation, such as an accumulation of ceasefire infringements – firing across the frontlines was already occurring shortly after the ceasefire was in place – new attacks by the Houthis or Iraqi militias, an ill-judged Iranian response to Israel's October airstrikes, or an Israeli decision to take advantage of an unexpected development in their favor. This final possibility is all the more likely if Netanyahu maintains his position as prime minister, with the new US president more willing to give the Israeli government carte blanche to do as it wishes without consequences. There will be more US sanctions for the IRGC and Iranian proxy groups, but not for Israeli settlers or politicians. US arms supplies to Israel will continue.

The arrival of Trump raises the prospect, moreover, of the Netanyahu government taking the opportunity to launch more extensive air attacks on the Iranian senior leadership, oil infrastructure, and nuclear program. Such action would be highly destabilizing and might yet lead to Iranian and Axis retaliation not only against Israel but also Western forces and Sunni Arab states in the region. This would probably involve further drone and missile strikes, as well as sabotage against Western oil interests, cyberattacks, assassination attempts, and terrorism in the region and beyond. Although this would not amount to an all-out land war between Iran and Israel – with no shared border, there is no place for their land forces to engage – it could lead to sustained aerial attrition between the sides, in effect, an ongoing 'air war' without an easy prospect of resolution. Regardless of who starts such a conflict, it would certainly lead to wider sanctions activity against Iran and its proxies by the US's allies, including the EU.

If tensions continue along the eastern Mediterranean coast, moreover, and perhaps, even if they do not, Iran might see the events of the last year as justification for pushing forward with the creation of a nuclear weapon. But given the potential consequences of a swift US military response to an attempted nuclear 'break out,' the regime is more likely to demure unless backed into a corner. Aware of its own weaknesses and instability at home, Iran's senior leadership knows that to go too far might put the regime in peril.

What could persuade them otherwise, however, could be outside support from a powerful ally, such as Russia, who could provide direct technical assistance to the Iranian program and reduce the risks of direct Western military intervention. For this kind of support, though, Russia will demand a higher price than drones and missile supplies, possibly including more direct Iranian involvement in Ukraine, along lines similar to that provided by North Korea. All things considered, Iran's leadership would probably see such a trade as too dangerous and costly, and Russia's bruising experience in Syria would also give it pause for thought about further Middle Eastern adventures.

One final note of hope is the possibility that the 'wildcard' return of President Trump, combined with Iran's own perceptions of its weakness and vulnerability, might yet lead to a diplomatic breakthrough. Trump is known to enjoy making big gestures and defying expectations, as he showed by undertaking face-to-face talks with Kim Jong-Un of North Korea in his first term. It is probable that at least back-channel talks about a 'grand bargain' between the US and Iran will be attempted, but given the entrenched interests and enduring enmities involved, any early agreement seems improbable.

What does this mean for me?

- International payments are the lifeblood of the Iranian shadow economy and are fundamental to its clandestine activities. If you work for a payment service provider (PSPs) with potential exposure to trading intermediaries, logistics firms, small financial institutions, or charities in Middle Eastern or East Asian markets such as UAE or Hong Kong, you will need to review the levels of risk that you might face from the activities of Iran and its partners. This is the case for both fiat and crypto-based service providers, as Iran and its partners, while still using tried-and-tested methods, are open to innovation.
- If your firm has exposure to trade or trade finance in those regions, or a substantial book of small- and medium-sized trading clients, you should also give special attention to potential sanctions' evasion and TBML risks.
- To best insulate your firm from sanctions, terrorist financing, and money laundering risks, you need to have extremely robust but flexible ongoing customer due diligence, drawing on the best risk information available. This means not only up-to-date sanctions and PEP lists but also adverse media information that can help identify high-risk counterparties not yet designated by governments. It also means having agile transaction monitoring platforms that can be configured – and reconfigured – to match changing hostile state, terrorist, and criminal typologies.

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

East Asia

Alongside Eastern Europe and the Middle East, East Asia has remained one of the main centers of geopolitical tension in 2024. Two hotspots are of long-running concern. First is the Korean peninsula, where North Korea's idiosyncratic communist regime has continued to threaten its neighbor, South Korea, as well as Japan and these two countries' more distant ally, the US. Second is the adjacent East and South China Seas area, where China's communist regime has persisted in promoting claims to the self-governing island of Taiwan, several smaller island chains, and the surrounding waters. These claims, while historic, are now being more aggressively asserted, putting China at odds both with its neighbors and the US and its regional allies, such as Australia.

The Korean Peninsula

The challenge posed by North Korea (officially titled the Democratic People's Republic of Korea, or DPRK) is undoubtedly one of the most long-lasting legacies of the Cold War. Created in 1948, the country has been governed by a hereditary communist regime, the Kim dynasty, since its inception. Throughout its existence, the country's relationship with the US and its allies has been fractious. In 1950, the North attempted to overrun the South, leading to a US-led UN-sponsored military intervention and a conflict that lasted three years, concluding with an uneasy armistice in 1953. Since then, the US has remained a military guarantor to South Korea, much to Pyongyang's annoyance.

The North Korean problem

Following its defeat, North Korea proved itself to be one of the most erratic members of the international community, taking aggressive actions against South Korea and Japan, including kidnappings, terrorism, and assassination attempts against senior South Korean officials. Its self-proclaimed economic principle of Juche, or self-reliance, made it an economic basket case, which, somewhat ironically, also made it dependent at various points on its communist neighbors, China and the erstwhile USSR.

Source: HillNotes

This meant poverty for most of the country's citizenry, with available economic and financial resources devoted to supporting the regime elite – especially the Kim family – and the development of the North Korean military. The regime also dabbled in a range of illicit activities such as currency counterfeiting, drugs, arms and illegal wildlife trafficking, and money laundering – often in collaboration with organized crime – to generate income. This wanton bad behavior led to an extensive US sanctions regime against the North, tempered with occasional US diplomatic efforts that sought – unsuccessfully – to bring the country out of isolation.

Tensions rose considerably in October 2006, however, when the North detonated its first nuclear device, and the UNSC swiftly applied a widening range of sanctions that sought to constrain Pyongyang's ability to source, develop, or fund WMD or ballistic weaponry. This action – which had support from both China and Russia – pushed North Korea into developing an extensive and complex sanctions evasion and procurement regime, bearing striking similarities to that of Iran. It also pushed North Korean criminal money-making activities into overdrive, encouraging it to become one of the state pioneers of cybercrime, first in the theft or extortion of fiat currencies and then cryptocurrencies. The regime used these funds to continue its WMD and missile programs. Over the last decade, it conducted successive missile tests indicating an ability to strike South Korea, Japan, and US bases in the Pacific and, possibly, the US itself. In light of North Korea's ongoing conduct, other Western powers joined the US in imposing their own autonomous sanctions on North Korea, including the EU, UK, Canada, Japan, and Australia.

A brief hope for rapprochement with the West did emerge during the first Trump administration, leading to direct talks between the president and the North's leader, Kim Jong-Un, in 2018 and 2019. However, the talks failed to satisfy either side, and the brief opening was followed by a hiatus brought by the COVID-19 pandemic, a period during which North Korea closed its borders to the world.

2024

Friends reunited

Post-pandemic, North Korea has sought to rekindle its more traditional friendships with China and Russia, with some success. By the end of 2023, it was clear that China was turning a blind eye to Pyongyang's sanctions evasion, working with Russia to obstruct further restrictions on the North at the UNSC. Even more dramatic developments occurred in North Korea's relations with Russia. In 2022, Pyongyang provided vocal diplomatic support for Russia's invasion of Ukraine, and in 2023, it became clear that North Korea was supplying Russia with munitions and other material needed to prosecute the war. The growing relationship between the two sides was sealed with a face-to-face meeting between Putin and Kim Jong-Un in Russia's Far East in September, presaging further cooperation to come.

The ambitious scope of the North Korean-Russian partnership became evident throughout 2024. In March, Russia vetoed the renewal of the UNSC's Panel of Experts (PoE) on North Korea, a group tasked with monitoring the implementation and evasion of UNSC nuclear sanctions. Diplomatic and military ties between the two states also tightened further; Putin visited Pyongyang in June, where he lauded the North Korean leader's achievements, and in November, the two countries formalized a military agreement that required each to support the other if attacked.

Western officials continued to highlight North Korea's supply of weapons and munitions to the Russian war effort. According to a September speech by senior US diplomat Robert Koepcke, North Korea had sent at least 16,500 containers of munitions and other supplies to Russia in the previous twelve months. Further investigations by The Financial Times and RUSI, a think tank, published in March, and the Open Source Centre, a research group, published in November, suggested that Russia was paying for these munitions by supplying North Korea with oil in excess of that allowed by UNSC sanctions. Perhaps the most surprising development of the year, however, were rumors in October, subsequently confirmed by the US military, that over 10,000 North Korean troops had been sent to Russia. Later, reporting from the US military indicated that the troops were being deployed around Kursk, with reports of the first North Korean casualties appearing in late November.

Kim emboldened

The growing relationship between Russia and North Korea and the forbearance of China also emboldened the Kim regime to pivot back towards an aggressive stance toward South Korea, Japan, and the US. At the start of 2024, North Korea announced that it would no longer seek "reconciliation and reunification" with the South, a move that some Western observers interpreted as a sign of hostile intent and potential preparation for war. Later, in October, Kim threatened to destroy the South with nuclear weapons if attacked. Although neither an invasion nor nuclear attack South resulted in 2024, other aggressive actions continued.

Some of these, including the dumping of waste and trash in South Korea using balloons, were faintly comical.

Others, however, were much more threatening, including a failed attempt to place a military satellite in orbit in May and several missile tests, including an apparently successful intercontinental ballistic missile (ICBM) launch in October.

North Korea's cyber campaign also continued. According to a media report in May, the soon-to-be-disbanded PoE had confidentially informed the UNSC that North Korea had laundered $147.5 million of previously stolen cryptocurrency through US-sanctioned crypto 'tumbler' Tornado Cash in March. The PoE also claimed to have said that the North had conducted 11 cryptocurrency thefts worth $54.7 million in the first few months of 2024. They suggested – in line with reporting from US law enforcement agencies – that many of these thefts could have been conducted by North Korean hackers living abroad or even working remotely as IT specialists for unwitting companies in the US.

Western responses

As noted in the previous section on Russia, North Korea's supply of 'arms for oil' in support of the Russian effort in Ukraine was a major area of Western sanctions activity in 2024. The major round of joint Western action on Pyongyang's support for Russia came in May, when the US, UK, Canada, Australia, and New Zealand imposed a range of measures on individuals and entities involved in illicit trading. However, given the already substantial sanctions regime on North Korea, many of the delegations focused more on Russian individuals and entities than those of North Korea. However, some North Korean entities were designated.

The UK-listed North Korean shipping firm Paekyangsan Shipping, which operated the North Korean flagged vessel Paek Yang San 1, was involved in facilitating arms and oil transfers. The EU also took more general action against North Korean officials, intelligence officers, and state trading companies in May, citing both North weapons proliferation and support for Russian aggression as grounds for doing so. This followed a number of North Korean designations in its 13th Russian sanctions package from February, which had included the North Korean Defense Minister, Kang Sun-Nam.

Western states imposed further designations on more familiar grounds as well. Weapons proliferation was an ongoing area of activity. OFAC listed six individuals and five entities based in China in July, which the US claimed were involved in the procurement of items to support North Korea's missiles and space programs. Chinese national Shi Qianpei was alleged to be the lead facilitator in a network overseen by a Beijing-based North Korean official, Choe Chol, who had previously been designated by the US in 2023 for weapons procurement activities. The UK also took more general action against North Korean WMD and ballistic missile development in January, March, and April, with designations that included North Korea's Academy of National Defense Science, General Bureau of Atomic Energy, Ministry of National Defense, and National Aerospace Technology Administration.

North Korea's illicit funding networks were targeted, too, particularly by the US. In March, the US and South Korea took coordinated action against six individuals and two entities, which they claimed to be key elements in North Korea's illicit financial network. These included several North Korean bank officials based in Russia and China, as well as a recruitment network led by the already US-designated North Korean Chinyong Information Technology Cooperation Company. According to the designations, Chinyong was using proxy firms in Russia and UAE to manage clandestine attempts to place North Korean IT workers based in 'laptop farms' in Russia, China, and Southeast Asia into remote working positions in third countries and the West. These workers were intended both to generate funds and gain access to sensitive systems. In associated action, the US DoJ announced various arrests, searches, and seizures in May and August 2024, under its DPRK RevGen: Domestic Enabler Initiative, designed to disrupt these illicit placements, with individuals arrested and charged, including both US and foreign nationals.

Besides sanctioning North Korea for its support for Russia and ongoing weapons procurement, the EU also designated Ri Chang Dae, North Korea's Minister of State Security, in July. According to the EU, Ri was responsible for human rights abuses and sexual and gender-based violence against women and girls. In tandem, the EU designated Onsong County MSS Detention Centre, one of the Kim regime's most notorious penal centers, where torture and other abuses were reportedly systematic.

Impact on North Korea

Sanctions have had a crushing effect on the North Korean economy, made worse by its self-imposed isolation, misguided economic policies, and incompetent state management. The North's GDP has thus remained a tiny proportion of the equivalent figure for the South. However, rather than this prompting internal reform or an attempt to normalize relations with the West, it appears to have encouraged the regime to pursue ever more repressive policies at home and hostility overseas. Rather than looking at its own poverty as a problem to be resolved, it has been treated as one to be accepted and worked around, regardless of the consequences. The regime has chosen to channel what resources it has into the support of the state and the military rather than the wider well-being of the civilian population, hoping that repression, isolation, and threats will enable its survival. While many Western observers question the logic of this in the long-term, believing that the regime will collapse at some stage, there is no immediate evidence that this is about to take place or that its prospect is an important element in the policy calculations of Kim Jong-Un.

Prospects for 2025

Considering the length of time North Korea has been a thorn in the side of the West, it would be a brave observer who would suggest anything other than 'more of the same' in 2025. The return of President Trump might lead to more unexpected talks aimed at resolving the countries' long-running disputes, but the failure of 2019, when expectations and hopes were high, suggests the chances of new talks succeeding are low, if not impossible. There is no indication that North Korea will be willing to denuclearize as the US and its allies wish or that the US will readily reverse its position. President Trump may love the unexpected, but he also hates what he sees as a "bad deal."

In fact, it seems much more probable that 2025 will see a worsening of Western relations with North Korea, although a military confrontation with the South and the US remains hard to foresee. The North will continue its aggressive rhetoric, launch test missiles and satellites, and perhaps even test a nuclear device for the first time since 2017. It will also harass the South, escalating its waste-dumping antics with the use of more dangerous substances. However, what seems most certain is that Pyongyang will keep moving closer to Russia. The arms-for-oil trade will be sustained and expanded, possibly covering a wider area of potential goods. The deployment of more North Korean military formations in the Russia-Ukraine war also seems likely, as does more direct Russian technical help in the North Korean missile and satellite programs. These developments will increase Western alarm and will prompt South Korea to boost its financial and material aid to Ukraine. However, current Western sanctions regimes against North Korea are already extensive, and the US and its allies will find few new economic and financial levers to pull to target North Korean activities. Most probable will be further targeting of the Russian end of the arms-for-oil trade and the involvement of individuals and entities based in neutral or third-country jurisdictions.

The most problematic of these third countries will be China, which has taken a selective approach to UNSC sanctions on North Korea for many years and allowed some North Korean individuals and entities to use the country as a relatively safe space for procurement and illicit financing activities. Chinese nationals and businesses have also often acted as Pyongyang's intermediaries, hiding North Korea's hand. The most obvious next step for Western countries, therefore, is to target clandestine North Korean networks in China more harshly, and this will dovetail with the negative attitudes of the incoming US administration towards Beijing. This will undoubtedly annoy China, too, although any response is likely to be tempered by Beijing's own concerns about North Korea's erratic and provocative behavior, especially its military relationship with Russia.

What does this mean for me?

- You are unlikely to see any dramatic changes to the UN, the US, or other sanctions against North Korea in 2025 in either a positive or negative direction. However, Western countries and jurisdictions with less extensive sanctions regimes than the US are likely to seek to start 'filling in the gaps' with new designations that match the US's longer-standing measures. Areas of US novelty are more likely to include more designations of firms and intermediaries used for North Korean sanctions evasion based in China, Hong Kong, UAE, and Southeast Asia.
- You should continue existing good practices on name and transaction screening, using agile platforms with access to up-to-date risk data. At the same time, you should pay close attention to the risks of North Korean sanctions evasion through third countries, both in terms of responding to new designations and taking a proactive approach to identifying risks in your existing client base through thorough due diligence reviews of high-risk clients (e.g., small- and medium-sized import/export firms) and the prudent calibration of transaction monitoring to identify unusual patterns of commercial and financial behavior.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

China

China, led by President Xi Jinping, is the greatest geopolitical problem for the West: it is an economically successful authoritarian state with a growing military. Its economy has boomed this century; Chinese GDP was nearly $18 trillion in 2023, according to the World Bank. It is, moreover, dominated by a communist elite, which has no sympathy with Western notions of democracy and civil liberties or the Western rules-based international order. It has repressed minorities such as the Uyghurs of Xinjiang at home, neutered the self-government of Hong Kong, a Special Administrative Region within China, and harassed and intimidated its dissidents and critics based overseas.

Moreover, China has shown itself to be a revisionist power in the international arena, with substantial territorial ambitions. Its 'One China' policy requires the return of the self-governing island of Taiwan to Chinese control, and its promotion of what has been called 'The Nine Dash Line' would redraw maritime boundaries in the South and East China Seas.

China also has an appetite for global leadership,

investing heavily in schemes such as the Belt and Road (BRI) trade initiative, which has given it significant leverage in the developing world, and evolving economic and political relationships with Western antagonists such as Russia and Iran. It has also developed its own Cross-Border Interbank Payment System (CIPS), overseen by the People's Bank of China (PBOC), China's central bank, which is intended to handle international payments and trade denominated in yuan. While not explicitly labeled as a rival to SWIFT, several Western observers have noted its potential to be used as a potential workaround in the event of future Russia-style sanctions against the country.

However, China is not only a problem for the West because of the difficulties it brings but also because of the opportunities it offers. The West has typically managed its relations with opponent states from a position of relative strength, allowing it to use a well-developed playbook of economic and trade incentives, military deterrence, and coercive diplomacy. China is far too big, too rich, and too important to isolate or browbeat, however. Much of the West, especially in Southeast Asia and Europe, is economically interdependent with the Chinese economy, and China itself, while increasingly assertive – and even aggressive – has managed to play a more subtle game than Russia on international diplomacy. While some examples of 'Wolf Warrior' diplomacy have been counterproductive, China has, on the whole, managed to walk a fine line between acceptable statecraft and egregious bullying. This has made it much more difficult for Western governments to frame China as an opponent against which it can apply its usual policies and remedies.

The West, and primarily the US, has therefore taken a carefully calibrated approach to China, focusing primarily on targeting economic and financial measures. Under both Presidents Trump and Biden, the US implemented export controls on American-made military and dual-use goods and technologies that go to China. President Biden's Creating Helpful Incentives to Produce Semiconductors Act (CHIPS), introduced in August 2022, included measures to incentivize the manufacture and development of semiconductors in the US – an act clearly aimed at 're-shoring' advanced technology development away from markets vulnerable to Chinese influence and interference. In a similar vein, the US also prohibited the use of Chinese technology in US Critical National Infrastructure (CNI), such as the 5G telecommunications infrastructure, and placed targeted financial sanctions on Chinese officials, institutions, businesses, and individuals allegedly involved in domestic suppression, or supporting the activities of rogue states such as Russia, Iran, and North Korea.

Until recently, US allies have been more reticent to use sanctions against China, but since the pandemic, several members of the Five Eyes alliance (consisting of the US, Canada, UK, Australia, and New Zealand) have taken action to limit Chinese commercial involvement in 5G infrastructures, and, alongside the EU, have imposed sanctions on Chinese individuals and entities allegedly involved in domestic repression. China has responded critically to Western designations, reforming its own counter-sanctions regime, although it has been applied lightly so far.

2024

Xi's balancing act

China can boast of several impressive accomplishments in 2024, not the least of which were the advances of its state space program. Despite China's image as a unified and dynamic regime, in 2024, it also confronted President Xi and the Chinese Communist Party (CCP) with various domestic difficulties. Despite a decade or more of anti-corruption campaigns, Xi's government continued to find new examples of graft, especially in the armed services.

While economic growth continued, the IMF expected China's GDP to rise by 4.8 percent in 2024, but it fell short of both China's 2023 growth of 5.2 percent and the CCP's own stated goal for the year of 5 percent.

Underneath the headline figures, moreover, there were further economic woes, especially in the property market, which has been declining since 2020. The market's ongoing weakness was exemplified by the final demise of Evergrande Group, a major Chinese real estate developer, which was liquidated in a Hong Kong court in January 2024. China also faced rising costs as a result of a combination of landslides, floods, and other natural calamities, with economic losses for Q3 2024 double that of the first half of the year. It also continued to experience a variety of man-made disasters, often resulting from the poor construction of buildings and infrastructure, such as the Meizhou expressway collapse in May, which killed 48 and injured 30. Reflecting a general sense of domestic malaise in China, research published in September 2024 suggested that the Chinese population was increasingly pessimistic about their financial prospects.

China had to deal with a complex environment overseas, too, with President Xi taking a 'goldilocks'-type approach, on the one hand aiming to show 'just enough' aggressiveness to assert its position as the US's leading global opponent, while on the other, seeking to avoid a direct confrontation. China continued to pursue improved economic ties with other revisionist powers such as Russia, Iran, North Korea, and Belarus, and closer military ties with Russia. President Xi also sought to cultivate a personal relationship with President Putin, inviting him to Beijing for two days of talks in May. The two pledged a "new era" of cooperation and a determination to challenge the US's global hegemony.

In addition, China sought to assert its territorial claims within the region. Taiwan's presidential election in January was subject to a massive Chinese disinformation campaign, and the Chinese military conducted several aggressive military exercises around the island, including one in October described as "punishment" for a speech by Taiwan's new President in which he promised to "resist annexation" by China. There were also ongoing clashes between China's Coast Guard and civilian fishing vessels and the Philippines' Coast Guard in the South China Seas. In November, China issued a set of "baseline" coordinates around the Scarborough Shoal, an area claimed by the Philippines. In another provocative move towards Manila, China carried out its first ICBM test since 1980, firing a missile over the northern islands of the Philippines into international waters in the Pacific.

In parallel, however, the country sought to burnish its credentials as a good international citizen. China promoted its Six Point Peace Plan to end the war in Ukraine, which was sponsored jointly with Brazil, although with little obvious positive impact. While standing back from direct involvement in the crisis in the Middle East, Beijing also sought to promote reconciliation between Palestinian factions, including Hamas and Fatah. China also made efforts to improve relations with its regional rivals. Throughout summer and autumn, it held talks with India intended to reduce tensions along their disputed Himalayan border, and in October, the two sides agreed to pull back their militaries in order to avoid future clashes. Separately, China sought to cultivate its southern neighbor, Vietnam, with which it has experienced an unpredictable relationship, inviting its new leader, To Lam, on a state visit in August.

Relations with the US

In line with its current caution, Beijing took a measured approach to the US and its Western allies, which they reciprocated. Building on the goodwill from a face-to-face meeting between Xi and Biden in November 2023 and the resumption of military talks in December, the two men spoke again on the phone in April, and diplomatic, economic, and military dialogues at various levels continued throughout 2024. Xi and Biden met again on the margins of the Asia-Pacific Economic Cooperation (APEC) summit in Lima, Peru, where Xi expressed his intention to work with the incoming US president, Donald Trump. Indeed, there have been several signs of constructive cooperation throughout the year, including climate change, financial stability, and AML. In the last instance, the US Treasury and PBOC announced in April that they would hold a "Joint US Treasury-PBOC Cooperation and Exchange on Anti-Money Laundering," which would "expand cooperation against illicit finance and financial crime," especially that linked to fraud and drugs trafficking.

Nonetheless, significant tensions remained, most obviously in the area of trade, where the US, EU, and other Western states claimed that China had been undercutting fair practices with market subsidies.

In September, the US finalized significant tariff increases on Chinese imports of electric vehicle (EV) batteries, solar cells, critical minerals, and semiconductors, which were originally announced in May. The EU also imposed tariffs on EVs in July. China said it would take "all necessary actions" in response to the US measure and announced a 39 percent import tariff on all EU brandy in October.

The Biden administration also took China to task over long-running issues, including Beijing's threats to the autonomy of Taiwan; its apparently lax attitude towards the enforcement of North Korean sanctions evasion; ongoing fentanyl precursor smuggling to the Americas; domestic human rights and civil liberties abuses; Chinese cybercrime; and increasingly, China's support for Russia during the Ukraine war.

However, much of the US's tough approach to China remained rhetorical, with President Biden and Secretary of State Anthony Blinken making public statements highlighting and condemning the role Chinese businesses had played in supporting the Russian military-industrial complex. Speaking in April, Blinken noted the role of Chinese businesses as major suppliers of machine tools and microelectronics to Russia, which are essential to its defense industry, and stated that "if China does not address this problem, we will."

The US, therefore, continued imposing export controls and financial sanctions on private Chinese entities and individuals linked to trade with Russia, a process that had already begun in 2022. Further designations occurred throughout 2024, usually as part of wider packages of anti-Russia or anti-Iran measures, with the US emphasizing Chinese firms' roles in supporting the procurement and development of drones by Russia and its allies. In April, for example, the BIS added two Chinese firms to its entity list, and in May, OFAC designated 20 Chinese and Hong Kong-based companies for providing "critical inputs" to the Russian war machine. Further Russia-related additions to the entity list and OFAC lists in August and October featured a significant number of designations of Chinese or China-based entities, including two companies involved in the production of Russia's long-range 'kamikaze' attack drones, the Garpiya series. In October, OFAC also designated two Chinese businesses involved in facilitating weapons procurement by the Houthis.

Alongside the problem of Chinese commercial support for Russia, the US revisited various other areas of previous action, especially China's programs of technological and military development. In March, for example, the BIS added 23 Chinese companies to its entity list "for acquiring and attempting to acquire US-origin items in support of the PRC's military modernization efforts."

The targeted businesses included major firms such as BGI Group, a genomics pioneer, and Inspur Group, a large cloud-computing provider. Other additions to the Entity List appeared throughout the year, targeting Chinese companies seeking advanced chips that could support AI military use cases. This included a mammoth package of 140 Chinese technology firms in early December, combined with the tightening of export rules on semiconductor manufacturing equipment and software. In October, the US Treasury issued a final rule that prohibited US investments in Chinese semiconductors and microelectronics, Quantum Computing, and AI. In September, the BIS implemented new general export controls on items used in the development of Quantum Computing items in order to protect US national security. While the controls did not mention China explicitly, most observers noted that it was the main target.

The Biden administration also took action in the cyber realm, with the US and UK jointly designating individuals and entities linked to China's state-backed APT 31 in March. According to the designations, APT 31, also known as Zirconium, had been a major player in Chinese cyber-espionage, hacking the emails of elected British politicians in 2021. In April, President Biden also signed the Protecting Americans from Foreign Adversary Controlled Applications Act into law.

This law required Chinese IT firm ByteDance to sell its social media platform, TikTok, within 270 days or face a US ban on the application. This followed bipartisan concerns that the sensitive data of US users of the application, including members of the military, were being exploited by Chinese state agencies. ByteDance said that if legal challenges to the US measure failed, it would likely close down TikTok in the US rather than undertake a forced sale of the platform.

In addition to national security concerns, the US imposed further sanctions linked to human rights abuses in China. Under the Uyghur Forced Labor Prevention Act (UFLPA), signed into law in December 2021, the US Department of Homeland Security (DHS) was empowered to establish a UFLPA Entity List, barring trade with companies that used Uyghur forced labor to produce commodities and products. Over 70 new listings of Chinese companies were made in 2024, focusing in particular on companies involved in textiles and clothes, agriculture and metals, and mining.

The rest of the West

While other Western countries took less extensive measures against China than the US, there was an increasing willingness to take a more confrontational approach to China's support for Russia. In July, following a summit in Washington, D.C., NATO's member states unanimously agreed that China had become a "decisive enabler" of Russia's invasion of Ukraine through its "no limits" partnership" with Moscow. In February, the EU's 13th package of Russia sanctions targeted four mainland Chinese companies for the first time. The EU's subsequent package in June designated a further six mainland Chinese companies, which were alleged to be involved in supporting Russian drone production and general military supplies. Both packages also designated several companies based in Hong Kong, following similar measures in earlier packages in 2023. The UK also imposed sanctions on entities in China alleged to be supporting the Russian war effort in June and November, along with other third-country businesses. As with the US and EU, the designations were focused particularly on the supply of machinery and microelectronic components used in drone production.

China's countermeasures

China overhauled its own autonomous sanctions regime in the early 2020s, and recent research indicates that in the first years of the decade, it became more willing to use such economic and financial sanctions than before. However, in comparison to the US, its deployment was much more narrowly focused on outside actions that were "meddling in Beijing's internal affairs" rather than the bad behavior of other states, as China analyst Francesca Ghiretti described it.

Nonetheless, 2024 saw an uptick in activity as the year progressed. China's Ministry of Commerce (MOFCOM) added several US defense companies to China's Unreliable Entities List (UEL) for supplying defense equipment to Taiwan in the spring, including General Atomics Aeronautical Systems and Boeing Defense, Space and Security. The ministry also announced that it would investigate the US clothing company PVH for potentially boycotting Xinjiang-produced cotton in September – a first for a clothing company. Separately, an analysis published by legal experts in September 2024 found that of the 100 individuals and entities sanctioned by China's Ministry of Foreign Affairs (MFA), around 60 had come in the previous 12 months alone, chiefly in response to perceived interference in Chinese affairs in Taiwan, Hong Kong, and Xinjiang. The growing numbers of designations suggested China's greater willingness to take countermeasures against the US. In December, Beijing reacted swiftly to the newly established US export controls on semiconductors with a ban on the export of gallium, germanium, and antimony – three critical minerals with military technology uses – to the US. This measure complemented more general export measures on dual-use aviation and space components announced in May, drone components announced in July, and a list of around 700 dual-use civilian and military items announced in mid-November.

A phony war?

2024 was thus another year of relatively controlled tension between China and the West. However, as we have seen, by year-end, China appeared to be increasingly willing to push back on some Western sanctions, especially where they were perceived to be related to Chinese sovereignty.

At the same time, it has been apparent that both sides have sought – despite some of their challenging moves – to keep matters in the realm of competition rather than conflict.

The US and its allies elected to take a gradual approach to sanctioning China's commercial support for Russia, and despite having the means to do so, President Biden held off applying secondary sanctions to Chinese banks facilitating sanctioned transactions with Russia. In fact, rather than taking advantage of this, several Chinese banks took the conciliatory – or perhaps precautionary – measure of limiting transactions with Russian clients in the spring. There were further media reports in December, moreover, that some major Chinese banks, including the Bank of China, were blocking payments to sanctioned Russian entities.

In addition, China's general dual-use export control measures were a double-edged weapon. Yes, the controls did limit the supply of Chinese technology to the US and other Western countries. However, at the same time, the restrictions placed limits on what could be supplied to Russia, as well as intermediary countries that might act as transit countries for sanctioned goods. While the key to these controls' effectiveness would come in their implementation and enforcement, they did at least suggest some willingness on China's part to respond to Western concerns, however obliquely.

Prospects for 2025

Considering the array of domestic concerns facing President Xi, it seems probable that China will continue its global balancing act in 2025: on the one hand, asserting itself in the South China Seas, taking easy offense at Taiwanese and US behavior, and seeking to find ways to support Russia and other revisionist states, and on the other, preferring symbolic or carefully calibrated responses which avoid military confrontation with the US or its allies. A blockade or even invasion of Taiwan in 2025, therefore, seems improbable, absent a major provocation by Taiwan or some other unpredictable 'black swan' event. This, at least, is likely to please the new US president, who made his preference for peace over war a major plank of his election campaign. More likely than a military confrontation with China will be periodic outbursts by Trump directed at US allies for not spending enough on their own defense.

Although a military crisis seems unlikely, the year will continue to provide numerous challenges, and whether Xi will be able to walk his tightrope successfully in the economic and financial spheres is uncertain.

Despite Trump's stated respect for Xi, he has an extremely negative view of China's trade practices and has expressed a determination to correct what he sees as economic imbalances using tariffs. He will also have several China hawks in senior positions, such as Secretary of State nominee Marco Rubio, as well as a strong anti-China lobby in the House of Representatives, encouraging him to take a tough line on Xinjiang, Tibet, Hong Kong, and other issues China deems to be none of the US's business. While Trump's first action against China will come with tariffs, past precedents suggest he will also be willing to use sanctions liberally. China should also be prepared for the US to take an even tougher line on Chinese commercial and financial support for the Russian war effort in Ukraine, partly to coerce Russia into a deal but also to drive a wedge between the "no limits" partners. There will almost certainly be many more designations of Chinese firms and entities and probably some secondary sanctions against smaller Chinese banks. The US will also put pressure on its European allies to take a tougher approach to restrict Chinese access to military and dual-use technologies, potentially as part of a 'quid pro quo' for sustained US engagement in European affairs. This suggests that the EU, UK, Canada, and others will start to expand the scope of their restrictive measures in line with the US approach, although they are unlikely to wish to go as far, given their greater economic dependence on China.

China too is more likely to respond in kind to Western sanctions with sanctions of its own. Yet, it seems probable that even if the scope, intensity and range of Chinese sanctions application increases in 2025, it will still lag far behind the US and its allies.

What does this mean for me?

- If your firm operates in the Asia-Pacific region, the trajectory of US-China relations in 2025 suggests a pattern similar to recent years. You will need to be prepared for more US sanctions and export controls against Chinese businesses, especially those operating in advanced technologies. You should also be prepared for the possibility that the US will designate several smaller Chinese financial institutions over systemic breaches of Russia sanctions and that the EU, UK, and other Western states will expand their range of sanctions against China, both to pressure China and appease the US. You should also expect to see more changes in Chinese sanctions next year, which might cause some conflicts of interest between firms with Western and Eastern interests.

- You should, therefore, prepare your organization by ensuring that you have access to comprehensive risk data and name-screening platforms that react to list changes in real-time. You should also review the risks you might face from direct or correspondent relationships with Chinese financial institutions, and prepare your response in advance for any future US measures against Chinese banks and financial institutions.

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

Regional review

The world's attention has been held once more this year by the events in Eastern Europe, the Middle East, and East Asia. However, they have not been the only regions to witness geopolitical developments or changes to sanctions regimes, and these are reviewed in brief below. Interestingly, it has been in several of these areas that some level of cooperation between Western countries, Russia, and China has continued at the UNSC, although collaboration was neither extensive nor enthusiastic.

Europe

The stability of the Balkans region has been a long-term concern of the international community, especially in the states of the former Yugoslavia. One of the greatest worries has been **Bosnia-Herzegovina**, a state made up of Serbian, Muslim, and Croatian communities, and one which fought a bitter and bloody civil war in the 1990s. In a rare show of unity, the UNSC unanimously voted to renew its support for the EU-led stabilization force in the country (EUFOR-Althea) for another year in November, in spite of Russian misgivings. The US also took designatory action against individuals linked to Milorad Dodik, the President of the Serbian province of Bosnia, known as Republika Srpska. Dodik is an avowed Serbian nationalist and has been subject to numerous allegations of corruption. OFAC's designations covered Dodik-linked associates and entities involved in attempts to disrupt the Dayton Peace Agreement, direct government contracts towards crony firms, and evade existing US sanctions.

A further area of Western concern was **Moldova**, in the eastern Balkans. In October and November, the current pro-Western President, Maia Sandu, was re-elected in the face of a strong challenge from a pro-Russian contender, Alexandr Stoianoglo, and in October, the country voted narrowly in favor of seeking EU membership. Worries remained in the West over ongoing Russian interference in the country's politics. In February, the EU sanctioned the Association of People with Epaulettes, an anti-democratic Moldovan paramilitary group that had incited public violence, a senior Russian FSB officer responsible for Russia's covert activities the Transnistrian region of Moldova, and a group of senior Moldovan media executives who were alleged to have undermined the democratic process in the country. In October, the EU further designated Evghenia Guțul, the separatist governor of the autonomous unit of Gagauzia in Moldova, as well as several of her political associates, and Evrazia, a Russian non-governmental organization (NGO) promoting Russian interests in Moldova, as well as the group's founder, Nelli Parutenco.

Africa

In recent years, the Sahel region of Africa (running roughly from the Atlantic coast of Mauritania and Senegal across to the Red Sea coast in Sudan) has been highly unstable. The region witnessed several military coups, failed and successful, and has become subject to the increasing influence and interference of the Russian private military company (PMC), formerly known as the Wagner Group (see section on Ukraine). But in 2024, the main anxiety of the international community in Africa was the civil war and humanitarian crisis in **Sudan**. Two key factions – the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF) – which had been fighting for over a year and a half, causing civilian deaths, a massive refugee crisis, and food shortages, continued their conflict. The UN assessed that the country was in the early stages of famine.

While not taking many specific new measures, the UNSC agreed to extend its sanctions against Sudan for a further year in September, and added two further RSF generals to its list in November. However, in early December, Russia vetoed a UNSC resolution that would have called on all parties to cease hostilities to allow humanitarian aid into the country.

The US also took its own actions on Sudan, which were designed to restrict the finances of both sides. In January, OFAC designated entities such as the RSF-controlled Alkhaleej Bank, the SAF company Zadna International, and the Al-Fakher Advanced Works company, used by the RSF to sell gold and buy weapons. Further asset freezes on companies linked to the factions were imposed in April. In October, the US also made two sets of designations for Algoney Hamdan Daglo Musa and Mirghani Idris Suleiman, senior leaders of the RSF and SAF, respectively, who were responsible for procuring weapons for their own sides. Further US designations in May and November targeted senior RSF leaders Ali Yagoub Gibril, Osman Mohamed Hamid Mohamed, and Abdel Rahman Joma'a Barakallah for targeting civilians and using sexual violence in the region of Darfur.

In 2024, the main anxiety of the international community in Africa was the civil war and humanitarian crisis in Sudan.

These US actions were coordinated with sanctions imposed by other Western authorities. In January, the EU used its new Sudanese regime for the first time, sanctioning six businesses supporting the arms trade enabling the conflict (including Zadna International), and in June, joined the US indirectly sanctioning RSF commander Barakallah, other senior figures from both the RSF and SAF and Ali Ahmed Karti Mohamed, the former Sudanese Minister of Foreign Affairs under the previous administration of President Omar al-Bashir. The UK also designated several companies and financial institutions that supported the finances of the RSF and SAF in April. In the same month, Canada created its own Sudan regime to target the militias' military and financial activities.

A further area of international activity was the long-running civil conflict in the **Democratic Republic of the Congo (DRC)**. In this complex situation, various domestic factions have been fighting periodically for many years, supported and opposed by irregular and government forces from neighboring countries such as Rwanda. In June, the UNSC unanimously voted to sustain UN DRC sanctions for another year. In July, OFAC designated the Congo River Alliance (known as the AFC) to seek to overthrow the DRC government. In parallel, the EU designated various militia leaders for human rights abuses, including two leaders of the March 23 Movement/Congolese Revolutionary Army (M23/ARC), leaders from the Rwandan rebel group, the Democratic Forces for the Liberation of Rwanda (FDLR-FOCA), and the Rwanda Defence Force (RDF). At the same time, the EU followed the US in designating the AFC.

The Americas

In the Americas, the situation in **Haiti** was of great concern to the UNSC, which determined in October that gang-led instability on the island continued to threaten international peace. UNSC sanctions on the island were thus renewed for another year. The US also imposed new individual sanctions: in August against Michel Joseph Martelly, a former Haitian president with links to drug trafficking, and in September, against Prophane Victor, a former member of the Haitian parliament linked to gangs and human rights abuses, and Luckson Elan, the current leader of the Gran Grif gang. In July, the EU sanctioned Kokorat San Ras, a Haitian gang that used sexual violence as a weapon, under its global human rights regime. In June, Canada also listed three Haitian gang leaders for criminal acts and human rights abuses.

Both the EU and Canada also took action regarding the troubled country of **Guatemala**. Despite Bernardo Arévalo's success in the presidential election of 2023 and inauguration in 2024, he continued to be undermined by forces within the country. In January, therefore, the EU created a new Guatemala sanctions regime intended to hold "accountable those obstructing a democratic transition following the 2023 general elections." As a follow-up in February, the EU listed several senior Guatemalan legal officials and a judge for seeking to obstruct the democratic transition. Canada also took matching measures under a newly created Guatemalan sanctions regime in February.

The US also continued to target authoritarian leftist regimes in the region. In 2023, the Biden administration had agreed to limit oil, gas, and mining sanctions against **Venezuela** following an apparent agreement by the Maduro government to participate in a free and fair democratic election. But when Maduro welched on this deal in April – blocking his likely opponent Maria Corina Machado from standing – the US reimposed oil sanctions, giving US companies 45 days to wind down operations. In response, PDVSA, Venezuela's state oil company, said it would increase its use of cryptocurrencies as payment for oil and other fuel exports.

In September and November, OFAC further designated several Venezuelan officials involved in the manipulation of the presidential election in July, which Maduro claimed to have won against Edmundo González, contrary to independent observations. OFAC also listed officials and others involved in the subsequent repression and abuse of Venezuelan protesters and democratic activists. Separately, the US took measures against the regime of Daniel Ortega in **Nicaragua**, sanctioning Wendy Carolina Morales Urbina, Nicaragua's Attorney General, and three Nicaragua-based entities, including a subdivision of the Training Center of Russia's Ministry of Internal Affairs, involved in domestic repression, and two government-linked companies, linked to illicit gold sales, in May.

Asia-Pacific

In Southeast Asia, Western states continued to criticize Myanmar's military junta for its repression of democracy and its use of extreme force against the Rohingya minority in the country's Rakhine province. To mark the three-year anniversary of the coup that brought the military to power in February 2021, OFAC designated two Burmese companies, along with senior managers of one of the firms, which were alleged to support the activities of the state-linked and already designated Myanma Economic Holdings Public Company Limited (MEHL). The companies' activities included the sanctioned purchase of foreign currency, the import of commodities, including oil, and a range of other manufacturing and logistical activities for the regime.

The UK also imposed new Myanmar sanctions in February on two divisions of Myanmar's armed forces,

allegedly involved in human rights abuses, and two state-owned companies. In October, the EU, UK, and Canada also implemented additional sanctions. These included an EU listing of the company Chit Linn Myaing Group (CLM), its founder, Colonel Saw Chit Thu, and several military associates who both support the regime and oversee a large criminal empire that included people trafficking and running scam centers. The UK and Canada also targeted entities supplying equipment and aviation fuel to the Myanmar military in response to the regime's use of airpower as a repressive tool. Australia, too, imposed additional measures on Myanmar in February 2024, including five entities linked to the regime's financing and military procurement.

Thematic review

Over the last decade, the international community, and especially Western governments, have become engaged in tackling issues not only at a national level but thematically too, and as a result, sanctions regimes for a range of different concerns – transnational crime, cybercrime, international terrorism, human rights abuses, corruption – have evolved to greater and lesser degrees in the US, EU, UK and elsewhere. However, as readers will have noted, these regimes have increasingly been used to target activities linked to broader geopolitical and national security issues linked to specific states. In the case of Russia, for example, it is growing harder to separate out what state and non-state-linked criminality is and the extent to which that crime is being undertaken for private or patriotic motives. It is possible, therefore, that in some of the cases discussed below, there are links to wider security concerns that have not yet become apparent to the public.

Transnational organized crime

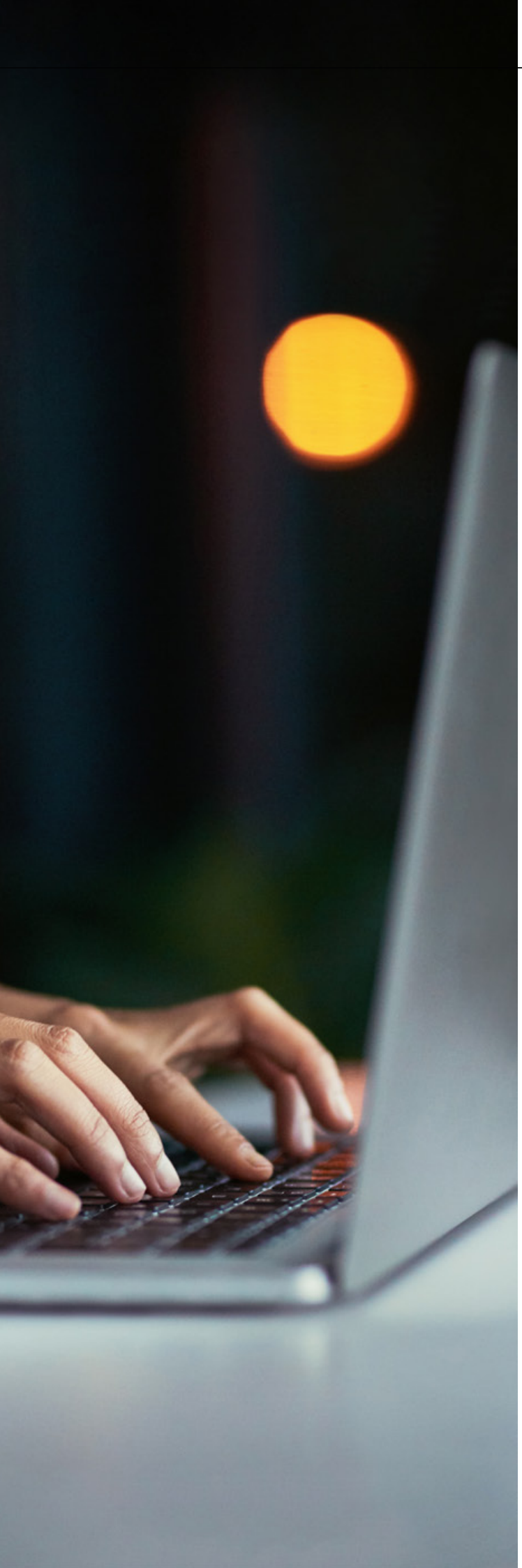
OFAC had another active year targeting the activities of the **cartels** based in various Latin American jurisdictions, especially those involved in the flow of fentanyl from **Mexico** directly into the US market. Designations included Juan Carlos Banuelos Ramirez, a leader of the Mexican Cartel de Jalisco Nueva Generación (CJNG) and two linked Mexican companies in July, and a further group of nine Mexican nationals associated with CJNG in November. OFAC also sought to undermine the cartels' illicit financing efforts, sanctioning operatives of the Sinaloa Cartel involved in the 'Black Market Peso Exchange' (BMPE) scheme, a TBML-based money laundering framework, in March, and Sinaloa-linked operatives of a China and Mexico-based money laundering scheme in July. Further OFAC efforts sought to tackle the Mexican cartels' increasing diversification into other areas of criminality. This included designations of several Mexican accountants and companies linked to timeshare fraud by the CJNG in July, designations of nine Mexican nationals and 26 Mexican companies involved in a CJNG fuel theft network in September, and designations of Mexican nationals linked to the Gulf Cartel involved in drugs smuggling, human trafficking and illegal, unregulated and unreported (IUU) fishing in November. The US also targeted the human smuggling network of Abdul Karim Conteh, a national of Sierra Leone based in Mexico, responsible for a global network of people smuggling flowing into the US.

The US took extensive action beyond Mexico, too. In neighboring **Guatemala**, OFAC redesignated the Los Pochos drug gang and linked companies in February for cocaine trafficking in cooperation with the Sinaloa Cartel and interference in Guatemalan politics. In July, OFAC designated the Lopez human smuggling network, while the US Attorney for New Mexico announced indictments against the leaders of the group, including its leader, Ronaldo Galindo Lopez Escobar. Further afield, OFAC also designated Tren de Aragua, a rapidly growing **Venezuela**-based crime group, as a transnational crime organization (TCO) in July. The group was alleged to be involved in a wide spectrum of criminality, including narcotics smuggling, human trafficking, illegal migration, gender-based violence, and money laundering. In **Colombia**, OFAC designated members of Colombia's Clan del Golfo (CDG), involved in both human and narcotics smuggling, in September. In **Ecuador**, it designated the Los Choneros gang and its leader, José Adolfo Macías Villamar (known as "Fito"), for involvement in narcotics trafficking with the CJNG and Sinaloa cartels, as well as their role in destabilizing Ecuadorian politics in February. This was followed in June by the designation of the Ecuador-based Los Lobos gang and its leader, Wilmer Geovanny Chavarria Barre (known as "Pipo"). In March, OFAC also designated Diego Macedo Gonçalves do Carmo, a member of Primeiro Comando da Capital (PCC), a large **Brazil**-based OCG involved in narcotics trafficking.

Outside of the Americas, in September, OFAC targeted Ly Yong Phat, a Cambodian businessman, his business, the L.Y.P. Group, and entities controlled by Ly – O-Smach Resort, Garden City Hotel, Koh Kong Resort, and Phnom Penh Hotel – for the **Cambodia**-based abuse of trafficked workers, and their exploitation in scam centers.

Cybercrime

The murky crossover in cybercrime between state and non-state activity has made it increasingly difficult to discern the difference between national security and



thematic designations. Nonetheless, non-state cybercrime groups continue to operate on their own behalf, including many of the Russian groups that dominate in the field of ransomware attacks. In January, the US, UK, and Australia jointly designated Alexander Ermakov, the hacker behind the ransomware attack on Medibank, an Australian health insurer, in 2022, and in May, the same coalition took action against the LockBit group responsible for LockBit ransomware, designating of the hacker group's leader, Dmitry Yuryevich Khoroshev. The US had already taken solo action against Lockbit in February, designating two members of the group. The EU also took action in June against several Russia-based cyber criminals who were involved in ransomware attacks on the health and financial services sectors in Europe.

Russia's ransomware groups were not the only targets, however, and in October, the US, UK, and Australia took joint action against members of the Evil Corp group and linked entities. Evil Corp is the developer of Dridex malware, which has been used to harvest customer log-in credentials from hundreds of financial institutions in over 40 countries, resulting in thefts worth more than $100 million. Russian crypto-based money laundering was also targeted. In September, for example, FinCEN identified PM2BT, a Russian cryptoasset exchange, as being of "primary money laundering concern," while OFAC designated its owner/controller, Sergey Sergeevich Ivanov. OFAC also designated Cryptex, another Russian crypto exchange registered in St. Vincent and the Grenadines. Finally, in December, the UK enjoyed a major operational success against a UK-based Russian money laundering ring that laundered funds partly through an underground crypto exchange. According to the UK's National Crime Agency (NCA), the group's scheme was used to launder billions of US dollars not only for organized criminals and hackers but sanctioned Russian oligarchs and Russian intelligence activities.

Beyond the Russia cybercrime nexus, OFAC targeted several other cyber actors. In May, it designated three Chinese nationals and linked businesses responsible for the malicious botnet 911 S5, which allowed criminals to use the internet connections of compromised computers as cover for their activities. In March and September, OFAC also designated several individuals and entities linked to the Intellexa Consortium, an umbrella term for an international, decentralized commercial offensive cyber group. The group was best known for its development of commercial spyware marketed as "predator." Amongst those sanctioned was the business's founder, former Israeli soldier Tal Jonathan Dilian.

Terrorism

Terrorist groups with links to Iran were the main focus of Western sanctions activity in 2024. However, other Islamist groups have been subject to action as well. In April, the US Department of State sanctioned leaders of Jama'at Nusrat al-Islam wal-Muslimin (JNIM), an **Al-Qaeda**-linked group in West Africa, for taking US nationals hostage. The Somalia-based insurgent and terrorist group **Al-Shabaab** faced the designation of three further senior group leaders by the UNSC in May, and in March, OFAC designated individuals and firms in an Al-Shabaab-linked financial network operating across the Horn of Africa, UAE, and Cyprus, which managed an extensive terror financing and money laundering scheme for the group. The US also continued to bear down on **ISIS**, designating several of the group's cyber security experts, human smugglers, and financial facilitators in Africa in January, June, and July, respectively. Separately, in coordination with Canada, OFAC designated the Samidoun Palestinian Prisoner Solidarity Network, a fake charity used to collect funds for the left-wing terrorist group, the Popular Front for the Liberation of Palestine (PFLP), as well as Khaled Barakat, one of PFLP's leaders.

The EU also took measures against both Al-Shabab, designating its member Ahmed Khaled Müller in January, and ISIS, designating its Sahel-based operative Mohamed Ibrahim al-Shafi'i Al-Salem in March. In addition, it designated the Al-Qaeda-linked and Sahel-based group Katiba Macina in the same month. Finally, the EU added the extreme right-wing group 'The Base' to its list in July – the first time it had designated a terrorist group of its kind.

Human rights and corruption

The US also used its Global Magnitsky regime to target state repression elsewhere. In September, OFAC listed Georgian officials and private citizens responsible for repressing peaceful protests in the country, and in December, designated three former Uzbek officials alleged to be involved in human trafficking, gender-based violence, and violence against children. The US also applied the Global Magnitsky regime to target corrupt practices, designating:

- **In January,** Alberto Pimentel Mata, Guatemala's former Minister of Energy and Mining, was arrested due to his alleged involvement in widespread bribery related to government contracts.
- **In March,** Zimbabwe's President Emmerson Mnangagwa, several associates, and three entities were sanctioned for involvement in gold and diamond smuggling and accepting bribes.
- **In June,** members of the Mohamed family, one of Guyana's wealthiest, along with the family company, Mohamed's Enterprise, and a government official, for public corruption.
- **In August,** Paraguayan tobacco company Tabacalera del Este for providing financial support to Horacio Manuel Cartes Jara, the former president of Paraguay who himself had been designated in 2023.

The UK also used its own anti-corruption regime, designating several corrupt Uganda politicians in April, and in November, the Angolan businesswoman (and daughter of a former Angolan president), Isabel Dos Santos, who allegedly misappropriated funds from the Angolan state oil and telecoms firms she previously headed. Also sanctioned were several of her associates and, in separate cases, the oligarchs Dmitri Firtash of Ukraine and Aivars Lembergs of Latvia.

Prospects for 2025

At any point, one or more of the aforementioned countries could explode into greater significance in 2025. Areas to watch particularly closely are Moldova, especially in the context of the war in neighboring Ukraine – possibly becoming a higher profile Russian target – and Sudan, where the humanitarian crisis is likely to grow to catastrophic portions if its current trajectory continues. More Western sanctions targeted on domestic subversives and Russian proxies are likely in the former, and a wider range of measures, possibly including UNSC resolutions, in the latter. However, given the precariousness of the situation in Sudan, it is likely that all members of the international community would prefer to avoid making things worse with poorly targeted measures.

The return of President Trump is also likely to mean a continuation and probable expansion of US sanctions against the cartels and Chinese money laundering groups supporting the drug trade in North America. Indeed, sanctions are likely to be a first rather than last resort, and the US will look to target not only local groups in Mexico and Guatemala but also those across wider Latin America, especially when their activities can be linked to drug trafficking and people smuggling into the US. The US is also likely to use designations to target more cyber criminals and their laundering infrastructures and to expand targeting against Islamist extremists, especially ISIS affiliates in Africa and Asia – a potential area of common cause with China and Russia.

Other Western sanctioning jurisdictions – the EU, UK, Canada, and Australia – are likely to use sanctions more readily to deal with specific international crises and address broader thematic challenges. It is notable how much more the EU, for example, has been willing to create new sanctions regimes to address the situations in Sudan and Guatemala. It is also notable how much more effectively Western states have begun to work together on shared areas of concern, such as the US-UK-Australia coalition tackling cybercrime. Much more of this kind of cooperation and coordination will come in 2025.

What does this mean for me?

- The significant focus on events in Eastern Europe, the Middle East, and East Asia has not meant that governments have abandoned other regional and thematic issues, and it has been notable how diverse, widespread, and enduring Western sanctions activity has been beyond the key hotspots in 2024. This is almost certain to continue and expand in 2025, driven by President Trump's preference for economic and financial over military measures and other Western countries' desire to exercise more global influence through pulling such levers. Sanctions lists are likely to grow and even increase in number as a result.
- This means that your team needs to have access to the most up-to-date listings and the most agile screening systems to ensure you do not get caught out by fast-changing geopolitical situations. You also need to give thought to how you might use valuable risk information, such as adverse media sources, to better understand the exposure you might face in regions not yet grabbing today's headlines.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

Back to beginning
Previous section
Next section

Regional regulatory trends

Global

Firms should continue closely following developments at the global AML/CFT standard setter, the Financial Action Task Force (FATF). During the FATF ministerial meeting held in April 2024, ministers reiterated their commitment to supporting the body in leading the fight against illicit financial flows via AML, CFT, and counter-proliferation financing (CPF) measures. They pledged to hold members to account for failing to implement the FATF standards effectively and called on countries to remain vigilant to threats to the financial system caused by Russia's war against Ukraine. Ministers indicated they would continue to work on promoting responsible innovation, ensure the digitalization of finance supports financial inclusion, look more closely at cross-border payments and central bank digital currencies, and prevent the misuse of virtual assets. The FATF will also continue to promote beneficial ownership transparency, asset recovery, and anti-corruption efforts, and work to understand proliferation financing, sanctions evasion, and complex money laundering schemes. The FATF will also increase the frequency and focus of mutual evaluation reviews (MERs), making them more risk-based.

The Mexican Presidency under Elisa de Anda Madrazo announced its priorities for the period covering 2024-2026. Key areas of focus include:

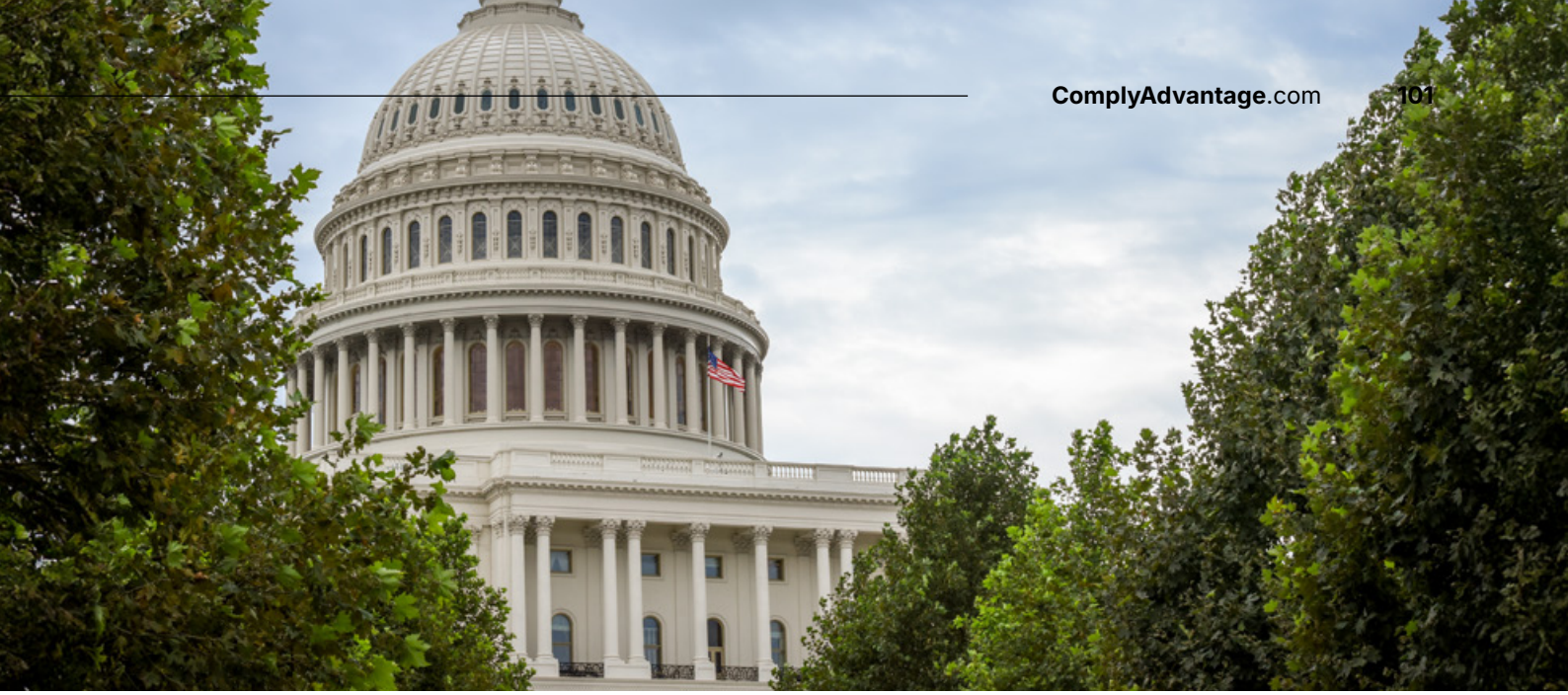
1. **Financial inclusion:** The FATF launched a public consultation on proposed changes to FATF Recommendation 1 and its Interpretative Note and Recommendations 10 and 15 linked to these changes and glossary definitions. These changes will promote proportionality, simplify measures, and provide a full understanding of risk, as part of the risk-based approach. The consultation closed on December 6, 2024, and the FATF has indicated that the revision and supporting guidance issued will be finalized in 2025.

2. **Strengthening the global network:** The FATF will work more closely with FATF-Style Regional Bodies (FSRBs) to promote inclusivity, collaboration, and diversity of perspectives. In recognition of the number of low-capacity countries on the FATF grey list, it will also mobilize resources to support low-capacity countries.

3. **Supporting the effective implementation of FATF standards:** The FATF will develop new guidance for the asset recovery space. Regarding beneficial ownership transparency, the FATF will facilitate sharing experiences on beneficial ownership registries and engagement with the private sector to promote greater understanding and buy-in. With regard to virtual assets, the FATF will look to accelerate implementation of its standards. Combating terrorist financing and proliferation finance will also be key areas for updated measures and assessments.

At the FATF October plenary, the FATF discussed future areas of work.

These include making changes to industry standards, reflecting the evolution of cross-border payments, and identifying emerging trends to identify the latest terrorist financing and proliferation financing risks and to help detect suspicious behavior and transactions to prevent online child sexual exploitation. Regarding key actors, the FATF is also reviewing its processes to ensure that countries do not misuse the FATF standards to target non-profit organizations (NPOs) and will continue to work on Designated Non-Financial Businesses and Professions' (DNFBPs') technical compliance with corruption guidelines. The FATF has also revised its national risk assessment guidance to help countries understand and mitigate their illicit finance risks, and will publish this soon. It is also working with data protection and privacy (DPP) experts, the private sector, and other international partners on information- sharing for AML/CFT/CPF and DPP.



North America

United States

The Corporate Transparency Act (CTA)

Following the re-election of Donald Trump, there is significant uncertainty as to the trajectory of AML/CFT and anti-corruption initiatives in the US. The Treasury last issued an updated National Money Laundering Risk Assessment in February 2024, stating that since the US is the world's largest economy, with a gross domestic product of $25 trillion, it is "particularly susceptible" to money laundering. Key threats identified include fraud, drug trafficking, cybercrime, the rise of professional money laundering via money mule networks, Chinese money laundering organizations and networks, sanctions evasion, corruption, human trafficking and human smuggling, tax crime, wildlife trafficking, and other nature crimes. Higher-risk vulnerabilities include the use of cash, money orders, pre-paid cards, peer-to-peer payments, legal entities and arrangements, virtual asset service providers (VASPs) that do not comply with domestic or international AML/CFT obligations, luxury and high-value goods, casinos, and online gaming, amongst others.

Some uncertainty remains around beneficial ownership transparency, a core part of the CTA. A federal district court in Alabama found the CTA to be unconstitutional as "it cannot be justified as an exercise of Congress' enumerated powers." The ruling has been challenged, and the case continues in the 11th Circuit Court.

There are also concerns about whether the CTA will be repealed after Donald Trump resumes the presidency. In the meantime, beneficial ownership requirements will kick in on January 1, 2025, requiring businesses to report information on who owns and controls the company to Treasury's Financial Crimes Enforcement Network (FinCEN). However, it has been recommended that firms report earlier. FinCEN has published a small entity compliance guide, which sets out who, what, where, and how reporting should be carried out. It also includes descriptions of what constitutes "substantial control" and how 25 percent of ownership interest should be determined. An individual meets the definition of substantial control if: (1) the individual is a senior officer; (2) the individual has authority to appoint or remove certain officers or a majority of directors of the reporting company; (3) the individual is an important decision-maker; or (4) the individual has any other form of substantial control over the reporting company. There are also more than 100 questions in FinCEN's FAQ document. Firms incorporated in the US and foreign firms with reporting obligations in the US should turn to these resources to clarify whether these obligations apply to them and how to meet beneficial ownership transparency requirements.

Real estate and investment advisers

As the new administration gets settled, FinCEN will continue implementing recently issued rules and regulations, expanding the scope of entities subject to the Banking Secrecy Act (BSA), including residential real estate transactions and investment advisers. FinCEN issued the final rules in August 2024 to safeguard these sectors from illicit finance and corruption. The Anti-Money Laundering Regulations for Residential Real Estate Transfers requires a new category of persons to submit reports and maintain records on certain types of financial transfers linked to residential real estate property deals involving legal entities and trusts.

The regulation details:

- **When a report must be filed:** A new category of report, "Real Estate Reports," must be filed when non-financed transfers are made to legal entities and trusts.
- **Who must file a report:** Certain persons involved in real estate closings and settlements.
- **What information must be provided:** Details specify information about the agreement, the reporting person, the transferor, the transferee, and beneficial owners of the transferee that must be included.
- **Associated timelines:** By the final date of the month or 30 calendar days after closing.
- **Record-keeping requirements.**

FinCEN has also issued a Residential Real Estate Fact Sheet and FAQs that firms should look to in order to understand who falls in scope of this regulation and how to comply with new requirements. The final rule will apply from December 1, 2025.

FinCEN extended the scope of BSA requirements to investment advisers registered with the Securities and Exchange Commission (SEC) and exempt reporting advisers that report to the SEC. The Anti-Money Laundering/Countering the Financing of Terrorism

Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers and Exempt Reporting Advisers introduces the obligations to have an AML/CFT program in place and submit suspicious activity reports (SARs) by adding certain investment advisers to the definition of "financial institutions" to regulations issued under the BSA. This was issued in response to the US Treasury's risk assessment that identified various illicit finance threats to investment advisers linked to foreign corruption, fraud, tax, and sanctions evasion. The rules amend different pieces of existing legislation and define "investment advisers" as any person registered or required to be registered with the SEC (adding certain exemptions). It further details rules for investment advisers, including the submission of currency transaction reports (over $10,000), record-keeping requirements, and information-sharing provisions under section 314(b). Finally, it sets out due diligence requirements when dealing with correspondent accounts for foreign financial institutions and private banking accounts. AML/CFT programs are subject to approval by the Board of Directors or Trustees and must include documented policies and procedures, independent testing by a third party, a nominated person responsible for the AML/CFT program, provisions for staff training, risk-based ongoing due diligence, understanding the nature and purpose of the relationship and ongoing monitoring and reporting. FinCEN has also issued a fact sheet that investment advisers should use to understand whether it applies to them and how. Firms are required to comply by January 1, 2026.

In July 2024, various US agencies, including FinCEN, the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency, issued an interagency notice of proposed rulemaking to amend AML/CFT program rules pursuant of the Anti-Money Laundering Act 2020 to also incorporate AML/CFT priorities. Key proposed changes include:

- Clarifying the purpose of AML/CFT program requirements to ensure institutions have compliant, useful, and "effective, risk-based, and reasonably designed" AML/ CFT programs.
- The requirement to have a risk assessment process as the basis for the AML/CFT program.
- Encouraging exploring technological innovations and approaches to preventing and detecting money laundering.
- The requirement to have a local compliance person physically present in the US responsible for the AML/CFT program.

These changes also include measures to address re-risking and financial inclusion, support feedback loops, and encourage innovation. This remains subject to ongoing consultation and review.

FinCEN has also issued alerts, reminders, and notices on the following topics: fraud schemes involving deepfake media targeting financial institutions; countering the financing of Hizballah; suspicious transactions associated with synthetic opioids; timeshare frauds associated with Mexican-based transnational criminal organizations; the illicit procurement of fentanyl precursor chemicals and manufacturing equipment; elder financial exploitation; Iran-backed terrorist organizations; environmental crimes; the use of convertible virtual currency for online child sexual exploitation and human trafficking; and Israeli extremist settler violence against Palestinians in the West Bank.

Canada

Canada will continue to enhance its AML/CFT national framework in line with its Anti-Money Laundering and Anti-Terrorist Financing Regime Strategy 2023--2026.

In 2020, the Criminal Intelligence Services of Canada estimated that up to CAD$113 billion was laundered in Canada each year.

As part of its strategy, Canada will look to improve coordination in the country across different sectors and across the world, improve operational effectiveness, close legislative and regulatory gaps on beneficial ownership transparency, and enhance regulation to manage financial crime risks associated with virtual currencies, mortgage lenders, and crowdfunding platforms. Canada's 2024 budget includes a section on "protecting Canadians from financial crime" to take further actions, including:

- Amending the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) to allow information sharing between private sector entities to detect and prevent money laundering, terrorist financing, and sanctions evasion.
- Allowing financial intelligence disclosures to provincial and territorial civil forfeiture officers to support asset seizures and strengthen the integrity of Canada's citizenship process.
- Extending AML/CFT obligations to factoring companies, cheque-cashing businesses, leasing and finance companies, and insurance companies when providing title insurance policies to real estate purchasers.
- Allowing for wider information-sharing when FINTRAC issues enforcement actions. An updated draft of the PCMLTFA was released in June 2024, which also extends reporting obligations to sanctioned property, with corresponding changes made to schedule two of the suspicious transaction report (STR) draft regulations. It also includes more stringent application requirements for money services businesses (MSBs) and a FINTRAC registration requirement for those providing acquiring services to white-label automated teller machines (ATMs).
- Amending the criminal code to allow for orders to be issued requiring financing institutions to keep accounts open during investigations, and for courts to issue repeating production orders for ongoing, specified information in accounts during criminal investigations.
- Amending the Income Tax Act and the Excise Tax Act to allow investigators to obtain warrants through court applications, simplifying evidence- gathering to fight tax evasion alongside other crimes.
- Providing $1.7 million over two years to finalize the design and legal framework of the Canada Financial Crimes Agency (CFCA), which is set to become Canada's leading enforcement agency. The CFCA will collate expertise to increase the number of money laundering charges, prosecutions, and convictions, and the seizure of criminal assets.
- Providing funding over five years to enhance the fight against trade-based fraud and money laundering by creating a Trade Transparency Unit in Canada's Border Services Agency.

What does this mean for me?

- A number of new firms are being brought into the scope of AML/CFT requirements in North America. Your team will need to ensure that your organization is able first to determine whether they are covered by regulation, and then able to build out AML/CFT programs to comply with those requirements. This includes having documented programs in place and introducing relevant technology to support the processing of customers and transactions, depending on how many customers you have.

- You may wish to develop programs with detailed work plans on how to introduce new customer due diligence (CDD), transaction monitoring, payment filtering, and sanctions checks (as needed for your operations), and how to manage these processes across your existing customer base.

- You should explore using both technology and outside technical expertise to document programs and carry out remediation on existing clients. 57 percent of senior financial crime decision makers we surveyed indicated that if they were starting from scratch, they would use either a single SaaS platform for customer or transaction screening and monitoring or a modular SaaS platform that allows for different modules to be turned on over time, both with data included.

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

Europe

The new EU AML package

The EU will spend 2025 implementing the many changes introduced by the AML package as it looks to make it harder for criminal networks to launder money or misuse corporate entities to support criminal activities.

In 2023, Europol found that 70 percent of criminal networks in the EU laundered funds and that 80 percent of misused legal business structures were linked to criminality.

The Council of Europe accepted the AML package in May 2024 to harmonize AML/CFT rules throughout the EU. The package now consists of three key pieces of legislation. These individual pieces of legislation will become operational over the course of the next four years.

At the regional level, Regulation (EU) 2024/1620 (AMLA Regulation/AMLA-R) establishes a regional-level supranational Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). The AMLA will have supervisory authority over high-risk financial institutions while working with national supervisors to ensure that obliged entities comply with AML/CFT requirements. AMLA will also coordinate with and support financial intelligence units (FIUs) and have a supporting oversight role in conducting peer reviews of supervisory standards and practices in the non-financial sectors. It will have the power to impose pecuniary sanctions on entities subject to supervision. It was decided that the AMLA would be housed in Frankfurt. AMLA-R will apply as of July 1, 2025 except for Article 103, which applies on December 31, 2025, and certain activities that came into effect in June 2024. It is anticipated that by August 2025, AMLA will have a list of selected obliged entities and begin direct supervisory activities by the end of 2026.

At the country level, Directive (EU) 2024/1640 details country-level requirements to "improve the organization of national AML systems" by setting out how FIUs and supervisors can better work together and maintain oversight over their AML/CFT frameworks at the national and regional level. The directive requires supra-national risk assessments to consider sanctions evasion and for countries to consider the AMLA's risk assessments, which will be published every two years. The directive further requires states to have central beneficial ownership registers, with new verification powers, that are accessible to FIUs, other competent authorities, and self-regulatory bodies. Bank statements will also be formatted across Europe alongside centralized bank account information registers containing bank account numbers and locations.

These should be made available only through a single point of access to FIUs. A separate directive has been adopted to give national law enforcement authorities access to this information. The Directive also introduced a single point of access to real estate information. New supervisory provisions were also introduced for firms operating under the freedom to provide services through agents, distributors, and other types of infrastructure, as well as around how to regulate financial and credit institutions that are part of a group. Countries are required to transpose the new AMLD by July 10, 2027 into national legislation. However, an amendment made around who can access beneficial ownership registry data comes into effect on July 1,0, 2025. Changes made to Articles 11-13 and 15 of the original AMLD 6 relating to beneficial owner registries come into effect on July 1,0, 202,6, and requirements included in Article 18 of the original AMLD 6 on having a single point of access for real estate information must be effective by July 10, 2029.

At the private sector level, Regulation (EU) 2024/1624 (AMLR) details requirements directly applicable to the private sector to prevent the financial system from being used to launder money or finance terrorism. AML/CFT requirements are extended to different types of entities, including VASPs, traders of high-value or luxury goods, dealers in precious metals and stones, football clubs and agents, investment migration operators, non-financial mixed holding companies, crowdfunding service providers, intermediaries and crypto-asset service providers (CASPs). The AMLR also sets more stringent due diligence requirements for occasional transactions, with a € 1,000 threshold for CASPs and occasional transactions below € 1,000 and additional beneficial ownership requirements, including introducing new requirements for foreign businesses where they enter into a relationship with an obliged entity directly, or indirectly acquire real estate, or acquire motor vehicles over € 250,000. It also introduces access to beneficial ownership data for persons, including civil society and media, that have a “legitimate interest” in it. It sets the frequency of ongoing customer reviews for high-risk customers at one year, and for all other customers at five years. The AMLR also introduces a € 10,000 cash payment limit and will become effective on July 10, 2027. It will not apply to football agents and professional football clubs until July 10, 2029.

The original fourth part of the AML package, which related to transactions – the Funds Transfer Regulation (FTR) (Regulation EU2023/1113) – was adopted in June 2023 and became applicable on December 30, 2024. It detailed information that must accompany transfers of funds and value for fiat and crypto transactions.

The EU payments landscape

On the payments front, the European Council has prioritized creating a fully integrated instant payments (IPs) market. Our survey of financial crime decision-makers across France, Germany, and the Netherlands showed the overwhelming majority of firms were making significant adjustments to accommodate the Single Euro Payments Area (SEPA) Instant Credit Transfer (ICT) scheme. 41 percent said SEPA ICT implementation required a "significant overhaul," while a further 49 percent said "moderate enhancements" were required. Regulation (EU) 2024/886, regarding instant credit transfers in euros, was updated in March 2024 and looked to provide uniform rules for cross-border IPs in euros to increase the adoption of IPs and open banking. It also contains additional requirements to manage fraud, money laundering, and sanctions related to IPs. The updated regulation includes new definitions, verification requirements for processing payments, and additional requirements related to the identification of discrepancies and screening for sanctions. For example, an instant credit transfer is newly defined as "a credit transfer which is executed immediately, 24 hours a day and on any calendar day." Payment institutions and electronic money institutions were also brought into the scope of the IP system by the regulation. To manage fraud and compliance with restrictive measures, it introduces the requirement to verify payees and screen for sanctions, as well as the requirement to have strong internal controls. Controls should include a risk map with mitigating measures and controls, documented procedures and controls that detail how outsourcing functions, agents, and branches are monitored and controlled, accounting and financial reporting procedures, CVs for persons responsible for control functions, a non-statutory auditor, an overview of group governance and the management and oversight body.

With regards to sanctions screening, the regulations specifically state that firms should not verify whether the payee (recipient) or payer (sender) is subject to sanctions "during the execution" of an IP but should be carried out soon thereafter. The regulations also introduce reporting requirements, including the number of national and cross-border transactions rejected due to sanctions, amongst others.

41% of financial crime decision-makers said SEPA ICT implementation required a "significant overhaul," while a further 49% said "moderate enhancements" were required.

Tiered implementation dates have been introduced as follows:

January 9, 2025

- PSPs based in a country whose main currency is the euro shall offer Payment Service Users (PSUs) the ability to receive instant credit transfers in euros.
- PSPs based in a country whose main currency is the euro should offer IPs at no additional costs.
- PSPs must comply with updated sanctions screening requirements.

April 9, 2025

- Transposition of amendments to PSD2 and the Settlement Finality Directive by countries.
- Submission of the first report by PSPs to national authorities on rejected payments due to restrictive measures.
- Countries must have in place rules detailing penalties for failure to comply with sanctions screening requirements.

October 9, 2025

- PSPs based in a country whose main currency is the euro shall offer Payment Service Users (PSUs) the ability to send instant payment transfers in euros.
- PSPs based in a country whose main currency is the euro shall offer verification of the Payee services.

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.

The SEPA rulebook was also amended. The SEPA ICT Rulebook 1.2 provides guidance on how to set up IPs within an organization. The updated rulebook was effective on March 17, 2024 to align with the migration of the SCT Inst Scheme to the 2019 version of the ISO 20022 standard. ISO 20022 is a universal financial industry message scheme to introduce a standardized approach and design in the exchange of electronic messages.

Two sections of the rulebook include exception processing flows for payment service providers (PSPs) to deal with fraudulent payments. The rulebook further stipulates that participants must fully comply with money laundering, terrorist financing, and sanctions regulations. While a public consultation on the 2024 change request to the rulebook is ongoing, a new version of the rulebook has not yet been issued to align with the changes made in the updated regulation.

An additional piece of payments legislation, the Payment Services Directive 3, was proposed by the European Commission in June 2023. While a final draft was anticipated in late 2024, it is likely the final version of PSD3 and associated regulations will be available in mid-2025, with countries o be given 18 months to transpose changes into local law. PSD3 includes measures to tackle payment fraud, including more stringent strong customer authentication (SCA) requirements, new rules for the authorization of non-bank PSPS, and other data protection provisions.

France

Two key developments for firms in France are the move to increase coordination on AML issues amongst different government bodies and clarification of politically exposed persons (PEPs). The Government in Council established an interministerial steering committee for the fight against money laundering and terrorist financing. The committee is charged with proposing to the government strategic national priorities in the fight against money laundering and terrorist financing, measures to mitigate money laundering and terrorist financing risks and related data protection issues, and report progress on the national strategy to fight against money laundering and terrorist financing on an annual basis.

With France's National Assembly politically deadlocked, unless there is a material change in the political makeup of the country, major legislative reforms look unlikely in the coming year. A re-run of parliamentary elections cannot be held until the summer at the earliest, with the only alternatives likely to change the status quo in the meantime being an early presidential election or a technocratic government that can oversee core responsibilities until a new vote.

Germany

Germany's Financial Crime Prevention Act came into force on January 1, 2024. The new law sought to establish the Federal Office to Combat Financial Crime (the Bundesamt zur Bekämpfung von Finanzkriminalität (BBF)) in 2024 with relevant powers around targeting money laundering, sanctions, and illicit financial flows. However, due to the changing political landscape in Germany, the proposed "super authority" has yet to materialize, and there is uncertainty about whether it will ever be. Federal elections will be held on February 23, and, based on polling, a change of government is likely.

BaFin has issued Consultation 06/2024 –-- Interpretation and Application Guidance on the German Anti-Money Laundering Act –-- which will replace previous guidance. Proposed amendments include additional provisions for crypto-asset service providers. The German Ministry of Finance has also shared details about Sanctions Enforcement Act II, which led to the establishment of the Central Office for Sanctions Enforcement to ensure more consistent and effective application of sanctions by boosting sanctions enforcement.

What does this mean for me?

- If your firm offers services in Europe, even if you are not incorporated in Europe, you must be fully aware of the various changes and requirements contained in the AML package. You must ensure that you update local policies and procedures and assess the impact that these changes will have on your operating environments.
- Where you have not already done so, plan for how to incorporate these changes into their AML/CFT programs. If you're newly subjected to oversight, you should ensure that you get the right type and level of technical assistance to develop effective AML/CFT programs suitable to the size and nature of your business.
- As new national authorities emerge, you should ensure that you follow any public statements and announcements, identify any changes that could impact you, and build these into your horizon planning assessments.
- If you're working in the payments space in Europe, you will need to ensure that you stay up to date with the many changes being introduced and that your policies and processes are updated to reflect these. You will also need to ensure that your transaction filtering and funds transfer monitoring systems are in place and calibrated to comply with timing requirements around payments. Your policies must also denote when and how to screen IPs for sanctions in a timely and suitable manner using appropriate technology and exception policies for dealing with fraudulent payments.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

United Kingdom

With a new Labour government in place, economic crime is expected to remain an area of focus in the UK. Key priorities for the government include clamping down on corruption, kleptocracies, and illicit finance by employing sanctions designations using the Global Anti-Corruption Sanctions regime to defend democracy and promote security at home and abroad. The National Crime Agency (NCA) has indicated that "it is a realistic possibility that over £100 billion is laundered throughout and within the UK in UK-registered corporate structures each year." The UK will continue to boost AML/CFT detection and prevention frameworks in line with its Economic Crime Act 2 and as it begins preparations for its FATF Mutual Evaluation in 2028. Companies House reform continues under the Economic Crime and Corporate Transparency Act (2023), with Companies House having powers to strike off companies formed under a false basis, authorize and check authorized corporate service providers (ACSPs) carrying out verification services, require identity information to be provided when incorporating a new company or appointing a new director or person of significant control (PSC), and require existing directors and PSCs to verify their identity on an annual basis by the end of 2025. It is also anticipated that the UK's Home Office will issue an updated anti-corruption strategy in 2025.

Firms will continue to contend with the reality of the authorized push payment (APP) fraud reimbursement regime that took effect on October 7, 2024. This requires payment processors to reimburse APP fraud victims within 5 days. The Payment Systems Regulator set the maximum reimbursement limit for victims of APP frauds at £85,000 for Faster Payments, with the Bank of England setting the limit for Clearing House Automated Payment System (CHAPS) payments to £85,000 also. These limits will be reviewed after 12 months. This creates new challenges for firms and also creates a new risk of fraudulent APP fraud reimbursement claims, requiring firms to have in place clearly documented and more stringent fraud controls, APP fraud claims procedures, and claims made.

The Financial Conduct Authority (FCA) issued a Dear CEO letter on October 7, 2024, setting out expectations on APP fraud reimbursement that all firms should review. It details that PSPs should:

- Have effective governance arrangements, controls, and data to detect, manage and prevent fraud.
- Regularly review their fraud prevention systems and controls to ensure that they are effective.
- Maintain appropriate CDD at the onboarding stage and on an ongoing basis to identify and prevent accounts from being used to receive proceeds of fraud or financial crime.

The FCA and PSR are expected to monitor compliance in 2025 with the APP fraud reimbursement regimes to identify prudential issues, conduct breaches, and inadequate systems and controls. They will also ensure the regime is working well to protect consumers against APP fraud without harming the broader payments system.

The FCA has indicated it will continue to take action to tackle scams, fraudulent websites, and illicit finance as strategic priorities. In November 2024, the FCA issued an updated guide on financial crime risks, a key document for all firms subject to supervision in the UK. The changes look to clarify FCA expectations on consumer protection, requiring firms to consider whether systems and controls align with Consumer Duty. They also detail actions firms can take when evaluating or setting up financial crime systems and controls and help ensure costs are proportionate, encouraging firms to take more "more efficient innovative, technology-led approaches to activities," such as transaction monitoring. Key changes made include:

- Updates to the sanctions chapter.
- Requiring risk assessments to take proliferation financing into account.
- Supporting responsible innovation and technological approaches to transaction monitoring.
- Clarifying that the guide applies to crypto asset businesses registered with the FCA.
- Requiring firms to consider whether systems and controls align with Consumer Duty obligations.
- Relevant updates to reflect current realities.

The FCA also published a review of the treatment of PEPs. This followed an update to the Money Laundering and Terrorist Financing Regulations (MLRs) in January 2024, introducing an update to Regulation 35 detailing that a domestic PEP represents a lower risk than a non-domestic PEP. The review found that there was a need to clearly document the rationale for the risk rating allocated to a PEP, assess if the PEP classification was appropriate after the PEP has left office, improve communication with PEPs, clarify the meaning of senior management required for PEP sign-off, enhance staff training, and update policies to reflect UK legislating amendments on requiring domestic PEPs to be treated as lower risk than foreign PEPs. The FCA continues to host emerging RegTech, SupTech, and WealthTech solutions in its digital sandbox, and will continue to host TechSprints in 2025 to explore how emerging technologies, including AI, can support innovation to meet regulatory requirements. In our 2025 survey,

60 percent of compliance decision-makers ranked sandbox-based holistic testing of data, algorithms, and configuration and ease of use when ascertaining a RegTech vendor's capabilities.

Legal and accountancy services firms will also be subject to enhanced scrutiny in 2025. The FCA has indicated that it will work through proactive supervision via the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) to enhance standards in the legal and accountancy sectors. A recent OPBAS report found that supervision of Professional Body Supervisors (PBSs) is not consistently effective and will continue to focus on the legal and accountancy sector in 2025. The FCA will also continue to raise awareness of fraud, focus supervision on firms that are seen as being at higher risk for money laundering and fraud, and strengthen the supervision of sanctions systems and controls.

The NCA has issued alerts on sanctions evasion and money laundering in the art sector, including artwork storage facilities, sextortion, and cybersecurity. The NCA also published updated guidance on suspicious activity reports (SARs) and requested a defense from the NCA under the Proceeds of Crime Act (POCA) and the Terrorism Act 2000 (TACT), providing detailed guidance on the information needed by the NCA and an overview of the process.

What does this mean for me?

- Given the many changes being introduced into the UK's AML/CFT framework, you need to ensure that your firm has appropriate resources to carry out horizon planning activities, assess the impact of proposed changes, and plan on implementing changes into existing programs.
- You will need to ensure that proliferation financing is built into your enterprise-wide risk assessments, monitor for APP reimbursement scheme frauds, and understand the timing and types of beneficial ownership data availability.
- Your team should also carry out a gap analysis against the FCA's updated financial crime guide (FCG) to identify and close gaps against FCA expectations. You should also continue to refine and test AML/CFT programs to ensure that they remain fit for purpose.
- As firms like yours increasingly adopt technology, you should engage with the FCA to understand the potential opportunities and pitfalls.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

Asia

China

China continues to ramp up its anti-corruption campaign, with at least three top investment bankers being detained by Chinese authorities in 2024. President Xi Jinping's anti-corruption probe in the investment banking industry will continue into 2025, with ongoing arrests and detentions of financial professionals facing penalties, including death sentences and life imprisonment. Following unpublished guidance from Chinese regulators, state-backed brokerages are asking their investment bankers to hand in passports and request permission for travel. Travel approvals include additional measures such as a requirement to travel with a co-worker, pre-approved activities, and restrictions on certain activities. Regulators are also said to be scrutinizing IPOs and other capital-raising activities. China's US$1.7 trillion brokerage and capital-raising industries have faced severe slowdowns, leading to significant pay cuts of up to 25 percent of base salaries in some cases.

It is estimated that USD$154 billion is laundered in China each year, a figure that the country's leadership has disputed.

Nevertheless, China adopted a revised Anti-Money Laundering Law on November 8, 2024. The law aims to strengthen the rule of law in AML work and specifies that AML efforts should be conducted according to the law and that efforts should be compatible with risks.

The law includes the following key changes:

- **It aligns with national security and emphasizes that AML should support national security efforts.**
- **Introduces an all-crimes regime:** Expands the definition of money laundering to an all-crimes regime, stating that money laundering includes activity that conceals the proceeds and profits from any criminal activity, including terrorist financing.
- **Expands requirements to "specific non-financial institutions."** This includes real estate developers and intermediaries, accounting firms, law firms, and notary offices involved in real estate transactions, fund and securities management, and client fund-raising activity. Dealers in precious metals and gemstones are also included.
- **Required cooperation with know your customer (KYC) measures:** Requires all entities and individuals in China to cooperate with firms in meeting KYC obligations.
- **Introduces certain data protection provisions:** Requires persona information to be obtained as part of AML/CFT processes be kept confidential and that all data be handled appropriately and securely.
- **Extraterritorial application:** Extends the jurisdiction of the AML law to "any overseas money laundering and terrorist financing activity that occurs outside China but poses a threat to China's sovereignty and security, infringes on the lawful rights and interests of its citizens, legal entities, and other organizations, or disrupts the domestic financial order."
- **Introduced beneficial ownership regime and compliance requirements:** AML and other regulatory agencies will establish a beneficial ownership registry of legal entities and non-legal organizations.
- **Require enhanced due diligence:** Provides guidance on due diligence measures and extends CDD requirements for firms.
- **Ongoing customer monitoring:** Requires customer and transaction monitoring and record-keeping requirements.
- **Requirements for third-party service providers:** This Requires risk assessment of parties carrying out KYC due diligence on their behalf.

The law came into effect on 1 January 1, 2025.

Singapore

The government of Singapore has been very busy in 2024, and firms will be expected to incorporate the many enhancements being made to the national AML/CFT frameworks in 2025 into their AML/CFT programs. In 2023, Singapore disrupted the money laundering operations from overseas organized crime activities that have led to over S$3 billion in asset seizures, including property, vehicles, and assets in Swiss bank accounts. The Monetary Authority of Singapore (MAS) will likely monitor firms to assess whether they have updated their risk assessments and controls to align with those published in 2024 to deepen an understanding of money laundering and terrorist financing risk. These include the following:

- The Proliferation Financing (PF) National Risk Assessment and Counter-PF Strategy identified PF threats and high-PF risk sectors, including banks and maritime insurers, digital payment token service providers (DPTSPs) dealing with virtual assets, and corporate service providers, lawyers and dealers in precious stones and metals. It also details PF risk mitigation measures that firms should adopt, including compliance with United Nations (UN) Democratic People's Republic of Korea (DPRK) regulations and UN Iran regulations.
- The Money Laundering National Risk Assessment identifies key threats such as fraud and cyber-enabled fraud, organized crime, corruption, tax crimes, and trade-based money laundering. The higher-risk sectors include the banking sector, wealth management, digital payment token service providers, cross-border money transfer service providers (including remittance agents), licensed trust companies, the real estate sector, and precious stones and metals dealers.
- The Terrorism Financing National Risk Assessment highlights key risk areas, including money remittances and banks conducting cross-border payments, re-classification of digital payment token service providers to medium-high risk, and civil society organizations and dealers in precious stones, metals, and products remaining medium-low risk. The threat of raising and moving terrorist funds overseas remains "pertinent," with self-radicalized individuals posing the most serious threat to Singapore. Singapore remains vigilant of threats generated by the Islamic State of Iraq and Syria (ISIS), Al-Qaeda (AQ), and Jemaah Islamiyah (JI), as well as future threats posed by the Israel-Hamas conflict.
- The Money Laundering and Terrorism Financing Risk Assessment of Legal Persons highlights the vulnerabilities to misuse and obfuscate illicit money trails or assist in creating fictitious transactions and includes a list of the different types of legal entities in Singapore, which types can legally own property in the country, an overview of vulnerabilities, case studies, and controls – stressing the importance of beneficial ownership transparency – for each type of legal person.
- The Money Laundering and Terrorism Financing Risk Assessment of Legal Arrangements highlights that although legal arrangements are not frequently exploited, where they are, they tend to form part of broader complex corporate structures across multiple jurisdictions. They are at risk of concealing beneficial ownership of illicit assets.
- The Environmental Crimes Money Laundering National Risk Assessment identified higher-risk sectors that could be exposed to environmental crimes, including money changers, corporate service providers (CSPs), VASPs, and casinos.

The government of Singapore also issued the following national strategies, setting out its priorities for the years to come:

- **The National Anti-Money Laundering Strategy:** Sets out the approach to addressing money laundering and consists of three pillars: Preventing and detecting money laundering and enforcing actions against money launderers abusing Singapore's system. Actions that Singapore will be taking include: (1) Developing the National AML Verification Interface for Government Agencies Threat Evaluation (NAVIGATE) as a whole-of-government data sharing interface; (2) Establishing an AML sensemaking work group to maintain oversight over technology and capability development across government agencies; (3) Further deepening data sharing channels with private sector entities; (4) Clarifying requirements to build a consistent baseline for AML/CFT requirements across sectors; (5) Amending the Mutual Assistance in Criminal Mattera Act (MACMA) to improve cross-border legal assistance; (6) Enhancing the effectiveness of risk-based supervision; (7) Enhancing the beneficial ownership framework for legal persons and trusts, including by amending the Trustees Act; 8) Reviewing COSMIC (Collaborative Sharing of Money Laundering/Terrorism Financing Information & Cases); (9) Prioritizing law enforcement outcomes; and (10) Enhancing AML penalty frameworks in real estate and the legal sectors.

- **The National Strategy for Countering the Financing of Terrorism** refreshes the country's blueprint for developing future actions to address TF risk by adopting a five-pronged strategy that includes (1) Coordinated and comprehensive risk identification; (2) Strong legal and sanctions frameworks; (3) Robust regulatory regimes; (4) Decisive enforcement actions; and (5) International partnerships and cooperation.

- **The National Asset Recovery Strategy:** Singapore will continue to prioritize asset recovery in the future. The strategy sets out Singapore's approach to seizing assets as one of the key pillars of Singapore's AML regime, recognizing the transborder nature of money laundering cases in Singapore. The strategy focuses on detecting illicit funds, depriving criminals of ill-gotten gains, delivering recovery of assets for forfeiture and restitution, and deterring criminals from accessing Singapore's financial system.

Singapore also passed the Anti-Money Laundering and Other Matters Act on August 6, 2024, with a phased implementation approach, which started on November 14, 2024. The act enhances the ability of law enforcement agencies to pursue and prosecute money laundering offenses, including by sharing tax and trade data, enhancing processes to seize or restrain property, and aligning the AML/CFT framework for casino operators with FATF standards. It defines foreign environmental crimes, including illegal logging, illegal land clearing, illegal mining, illegal waste trafficking, and illegal wildlife trade, as a money laundering predicate offense in Singapore, tightens CDD checks for casino operators, and requires them to consider PF risk when onboarding customers and lowering the CDD checks to cover cash transactions or deposits over S$4,000.

MAS and the Infocomm Media Development Authority of Singapore (IMDA) have also introduced a compensation framework for fraud that firms must implement. They published a Shared Responsibility Framework (SRF) on October 24, 2024, for phishing scams that came into effect on December 16, 2024. The SRF details requirements for financial institutions and telecommunication companies (Telcos) to mitigate phishing scams and full payouts to scam victims where assigned duties are not met.

Additional duties include requiring financial institutions to have real-time fraud surveillance controls in place to identify unauthorized transactions. For payment service providers (PSPs), a kill switch should be made available alongside real-time notifications that will be required for new device logins, outgoing transactions, or higher risk activities such as a change of account contact details, increase in transaction limits, disabling transaction notifications, and adding a new payee. It also provides an overview of a four-stage operational workflow for claims, including a 'claim stage,' 'investigation stage,' 'outcome stage,' and 'recourse stage.' Firms must comply within six months. MAS will also be responsible for monitoring for fraud surveillance.

MAS recently set out its FinTech vision and explored how to benefit solutions from its digital sandbox at scale by "forming consortia with industry, with federal regulators, policymakers, coming together to solve problems." Over 20 financial institutions, industry bodies, standards setters, policymakers, and international organizations came together to solve problems for digital assets, and the regulator is promoting a collaborative approach to artificial intelligence (AI).

What does this mean for me?

- The changes may seem daunting if you're operating and offering services in Singapore. You should review the various risk assessments and update enterprise-wide and customer risk assessments and AML/CFT policies to feed down through the enhanced due diligence, ongoing monitoring and assurance testing controls.
- You will also need to enhance your AML/CFT frameworks to incorporate counter-proliferation financing (CPF) policies, processes, and controls, including carrying out a CPF risk assessment.
- The enterprise-wide risk assessment and customer risk assessment should also consider environmental crime risks and risks associated with legal persons and arrangements.
- You will also need to ensure that you build out a compensation framework for fraud. This includes onboarding technology solutions for enhanced fraud monitoring and building out notification mechanisms where these are not in place.
- Finally, your team will need to develop compensation processes in accordance with issued guidance and ensure they monitor management information to identify the usage of this safeguard. They will also need to carry out assurance testing, monitoring, and staff training on new fraud compensation processes and controls.

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

Australia

Against a backdrop where federal elections will be held before September 2025, Australia has taken much-needed steps to move 'Tranche 2' reforms forward, with parliament approving the measures on November 29, 2024. Australia has now held two rounds of consultations on the reforms, which were introduced to modernize Australia's AML/CFT national framework by expanding AML/CFT requirements to professional service providers. The reforms consist of the following three components: (1) Addressing ML/TF vulnerabilities in Tranche 2 sectors; (2) Modernizing digital currency and payment technology-related regulation; (3) Simplifying, clarifying, and modernizing the AML/CTF regime to reflect changing business structures, technologies, and illicit financing methodologies.

Five separate papers were issued as part of the consultation, and four industry-specific papers provided information to businesses being brought into the scope of the regulation.

The professional services companies covered include real estate professionals, professional service providers, dealers in precious metals and precious stones, and digital currency exchange providers (DCEPs), alongside traditional remittance and financial services institutions. Paper five details proposed reforms to the AML/CFT regime. These include clarifying appropriate risk mitigation measures, establishing a 'business group' concept to help manage group risks, requiring reporting entities to assign each customer a risk rating to determine levels of CDD, lowering the CDD threshold for gambling service providers from AUS$10,000 to AUS$5,000, and updates to the tipping off offense. The government has indicated that firms should maintain internal controls through proper governance and a robust compliance culture. The Financial Transaction Reports (FTR) Act will be replaced by the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) 2024 Act.

AUSTRAC released two risk assessments on July 9, 2024:

- The Money Laundering in Australia National Risk Assessment identified illicit drugs, tax and revenue crime, and government-funded program fraud as posing the highest threat of money laundering. It further found that money launderers continue to move funds via traditional methods, including cash, banks, luxury goods, real estate, and casinos in spite of the emergence of digital channels.

- The Terrorism Financing in Australia: National Risk Assessment identified self-funding and fundraising via social media, communications apps, and crowdfunding platforms as high risk for raising terrorist funds, and the banking system, particularly retain banking, remittance service providers, non-bank online payment service providers, and digital currencies as higher risk channels for moving terrorist funds.

AUSTRAC also issued a financial crime guide to help businesses identify and report suspicious activity related to criminal gangs targeting foreign students as money mules. AUSTRAC is also conducting a consultation to update guidance for customers who do not have standard identification. On September 26, AUSTRAC issued standalone suspicious activity indicators for the bullion sector, the pubs and clubs sector, the financial planners sector, the on-course bookmaker sector, the remittance service providers sector, the superannuation sector, the digital currency (cryptocurrency) sector, non-bank lenders and financiers, the casino sector and the online betting agencies sector, and the banking sector. It further enhanced guidance on employee AML/CFT risk awareness training, including examples of good and bad practices, and updated its customer identification and verification: an easy reference guide for reporting entities and reliance on customer identification procedures by a third party.

What does this mean for me?

- If you work for a firm that is being brought into the scope of the new act, you should contact AUSTRAC to review the relevant paper published for your industry. It contains examples of good practice under headings, including "What would this look like?" and should be taken into account when building out AML/CFT programs.

- You should also build indicators of suspicious activity for their relevant sectors into your training and awareness program and work with your technology vendors to ensure these are included in transaction monitoring systems.

- If you work for a DCEP, you will also need to develop plans to comply with updated travel rule requirements in due course and monitor any additional guidance issued by AUSTRAC.

- All compliance teams should review paper five, ensure they carry out gap analysis, and update their internal policies, processes, and technology systems to reflect changes. Firms must also ensure they carry out enterprise-wide risk assessments and build mechanisms to drive the customer risk assessment, CDD, and ongoing monitoring. Firms should look to the various risk assessments issued by AUSTRAC to inform their enterprise-wide and customer risk assessment policies and processes.

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

Emerging hotspots

Our survey of global financial crime decision-makers spotlighted a number of emerging hotspots around the world. The top four countries identified are explored further below. The following countries are jurisdictions under increased monitoring by the FATF, some of which are improving their AML/CFT frameworks.

Philippines: The Anti-Money Laundering Council (AMLC), the Philippines FIU, indicated that it is moving "closer to exiting anti-money laundering watchlists by 2025," which will pave the way for Filipinos to benefit from faster and cheaper remittances and other transactions. This follows an announcement by the FATF that the Philippines had closed out its agreed action plan items, including the risk-based supervision of DNFBPs, the enhanced risk management of casino junkets, new registration requirements for money or value transfer services (MVTS), enhanced beneficial ownership transparency and information access, implementing appropriate measures to the not-for-profit sector, and enhancing targeted financial sanctions frameworks for terrorist and proliferation financing.

South Africa: South Africa continues to make progress in getting off the FATF grey list, addressing 16 of its 22 agreed action items.

Progress is anticipated in investigating and prosecuting complex money laundering, terrorist financing, and cross-border money value transfer services, as well as ensuring beneficial ownership transparency and timely access to information. These actions must be completed by February 2025 to remove South Africa from the grey list. The Financial Sector Conduct Authority issued over eight fines and administrative sanctions in 2024 to numerous firms for AML/CFT failures.

Kenya: Kenya was added to the FATF grey list in February 2024 due to a lack of strategy and adequate investigations and/or prosecutions for money laundering and terrorist financing cases, limited supervision over the NPO sector, inadequate national risk assessment, poor PEP disclosures, inadequate regulation of VASPs, and an underdeveloped risk-based approach to AML/CFT.

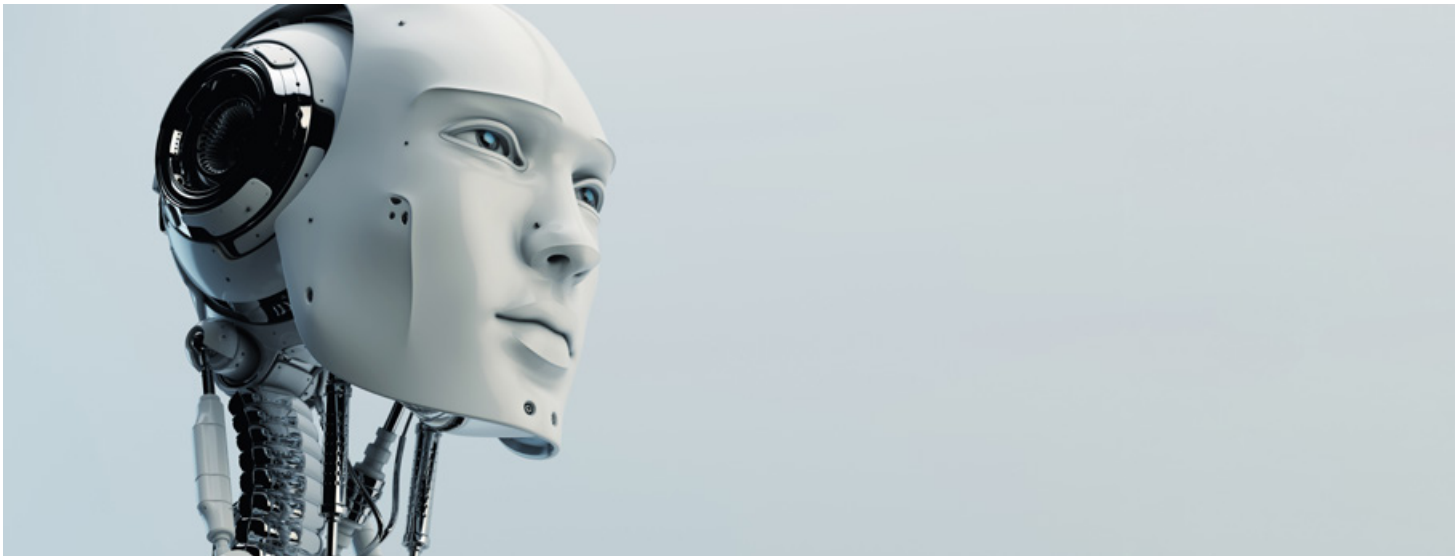
Nigeria: Nigeria continues to make progress in its program to be removed from the FATF grey list after being added in February 2023. Nigeria is anticipated to release an updated risk assessment in 2025 and monitor the implementation of VASP regulations and guidelines issued to MVTS providers. The country may also issue updated legislation to ensure compliance with FATF standards.

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

Source: ComplyAdvantage, The State of Financial Crime 2025

Back to beginning
Previous section

Regulatory themes



Artificial intelligence (AI)

In 'Spotlight on Financial Crime,' we highlighted ongoing concerns about how AI might be used by criminals, with a particular focus on the exploitation of generative AI (GenAI) and deepfakes. However, it is important to remember the economic potential of AI. According to the media outlet Forbes, quoting the data platform Statista, the global market for AI will reach $1,339 billion by 2030, growing by $214 billion in 2024 alone. A recent international survey by professional services adviser Deloitte found key use cases included:

- **Automation** of operational processes, resource planning, staff hiring, and code-writing;
- **Optimization** of platform reliability and downtime, workforce scheduling, and product pricing;
- **Predictive maintenance** of platforms and IT operations management (known as 'AIOps');
- **Predictive analytics** on market and client behaviors;
- **Personalization** of customer products and experience; and – of course –
- **Content generation** with GenAI.

All of these use cases have the potential to be applied to the operations of regulated financial institutions and significantly impact the effectiveness of financial crime compliance.

The improved pattern-recognition powers of machine learning algorithms, for one, can be applied to AML/CFT, fraud and sanctions identification and verification (ID&V), customer due diligence (CDD) checks, and ongoing monitoring and screening tools.

AI risks

Despite the potential of AI to reduce costs, improve customer service, and better manage risks, governments, regulators, and the private sector all recognize possible downsides. Systems fed with corrupted or incomplete data still make mistakes, a more sophisticated version of 'garbage in, garbage out,' especially when programmers do not understand the full range of inputs and parameters that would go into making the same decision in a human context. Systems fed with existing data can also become systematically biased in their interpretation of it, leading to prejudicial decision-making. In a different vein, AI systems also offer potential vulnerabilities that bad actors might be able to exploit. They are extremely attractive sources of large amounts of personal data, which can have high value in illicit markets. They also offer an opportunity to hackers who might wish to sabotage the outcomes of the system by meddling with its algorithms.

Global AI regulation

Among policymakers, caution has thus sat alongside optimism, leading to a debate on how best to mitigate AI's risks while ensuring appropriate and safe use. In doing so, the Group of 7 (G7) leading economies – the US, Canada, the UK, France, Germany, Italy, and Japan – have taken a leading role. At their summit in Japan in May 2023, the group initiated the Hiroshima Process, a policy dialogue that aims to promote "the safe, secure and trustworthy" use of AI through an agreed set of principles, a common code of conduct, and a shared policy framework. Subsequent to the summit, the G7 issued its proposed Comprehensive Framework in December 2023 and throughout 2024, and it has sought to develop and socialize its approach. In March 2024, the G7 Industry, Technology, and Digital meeting reiterated its support for the framework and called on other international organizations to work with the G7 to advance its implementation.

Of these, the Organization of Economic Co-operation and Development (OECD), an organization of 38 developed countries in the Americas, Europe, and Asia-Pacific, has responded most strongly to this call. Since the Hiroshima Summit, it has issued a stocktake on the global use of generative AI, a range of supporting papers on Data Governance and Privacy, Emerging Critical Risks, and Truth Testing, and a G7 Toolkit for Artificial Intelligence in the Public Sector. The UN has been somewhat slower in response, although the UN General Assembly adopted draft resolutions on the regulation of AI in March and July 2024 – one led by the US, another by China, but both supporting the other – and in September, the UN's High-level Advisory Body on AI issued a final report on AI governance, both of which were broadly aligned with G7 and OECD thinking. However, none of these government-led efforts so far equates to a binding legal or regulatory requirement for any individual government.

Beyond inter-governmental discussions, other global efforts to bring a coherent approach to the use of AI have developed in more practical areas.

The International Organization for Standardization (ISO), a non-governmental group bringing together national bodies responsible for technical standards and certification in technology and manufacturing, worked for several years with the International Electrotechnical Commission (IEC) to develop a set of standards for AI. This process led to the publication in December 2023 of ISO/IEC 42001 (ISO 42001), which offers organizations guidance on the design and implementation of AI systems that satisfy many of the fundamental requirements noted above, such as security, data privacy, and explainability. But – as with efforts in the global political arena – the ISO 42001 standard is not mandatory or legally binding, even if it is increasingly seen as a 'gold standard' within the private sector for the implementation of AI.

Regional developments

While there is a clear international direction of travel on AI governance – broadly shared across many countries – it needs to be emphasized that much of what has been agreed so far has answered the easiest questions. It is hard to disagree, for example, with the need for AI to be secure or fair. The more challenging question is how governments and regulators go about making this a reality is much harder, and on this, there is not yet a global consensus.

North America

In the US, there is no settled national approach to the governance of AI. At a federal level, several pieces of legislation and executive orders have been introduced that tackle some aspects of AI governance. In 2020, Congress passed the National AI Initiative Act, which created the National Artificial Intelligence Initiative Office to support AI development, and in September 2022, the White House issued its Blueprint for an AI Bill of Rights, providing guidance on the fair and ethical use of AI systems. The White House also issued an Executive Order (EO) titled The Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence in October 2023, focused on the development of AI standards in federal agencies including the watermarking and authentication of government content. Despite some successes in its first year of implementation, including voluntary agreements by parts of the private sector to align with the EO, many players in the world of 'Big Tech' did not follow the federal government's lead.

2024 has seen further disparate developments. In May, a bipartisan Senate working group issued a "Roadmap for Artificial Intelligence Policy," which noted the importance of various aspects of AI, including leveraging innovation, protecting workforce rights, privacy, and transparency. Separately in June, the Senate Committee on Commerce, Science, and Transportation, which had held hearings on AI transparency in September 2023, agreed on a raft of nine pieces of AI-related legislation for consideration by the full Senate in a future legislative session. Nevertheless, neither of these developments were intended to provide a comprehensive AI package.

Indeed, the then-Democratic Senate Majority Leader, Chuck Schumer, noted that the Senate had no intention of waiting for a comprehensive federal package and would consider AI bills on a case-by-case basis. In the House of Representatives, a further nine bills on AI-related legislation – focused on development, funding, and deployment, rather than regulation – were passed by the Science, Space, and Technology Committee in September 2024, but these bills seemed unlikely to go to the full House in 2024.

Various states have also passed or begun considering their own AI legislation in recent years. As of September 2024, according to the National Conference of State Legislatures (NCSL), 48 states and jurisdictions within the US have introduced AI-related bills, and 33 will have enacted them by the end of the 2024 legislative session. Those passed have included the Utah Artificial Intelligence Policy Act, which placed disclosure requirements on firms using generative AI with their customers, and the Colorado AI Act, which will come into force in February 2026. The Colorado Act covers a wide range of issues around potential 'algorithmic discrimination' in areas such as insurance, financial services, health, welfare, and employment and is seen by some observers as a potential model for other states.

Nonetheless, not all state-level legislation has enjoyed a smooth passage. In California, a bill providing for extensive safety testing of AI models and broad legal liability for AI developers, passed by state legislators, was vetoed in September 2024 by Governor Gavin Newsom, following lobbying by major technology firms. As the controversy following the decision revealed, a fundamental tension remains in US society between the desire to promote economic dynamism and to protect the rights of individuals. As yet, a sustainable balance has not been found.

Much like the US, Canada lacks a comprehensive legal and regulatory framework for AI, although, again, much like the US, several federal laws with some relevance for privacy and security standards already exist, such as the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA), passed in 2000. Other statutes on personal data and privacy at the provincial level in Quebec, Alberta, and British Columbia also have some implications for AI.

However, where Canada does differ from the US in the direction of travel, it is currently taking on AI, which is more clearly towards a unified framework. In June 2022, the Canadian government introduced an Artificial Intelligence and Data Act (AIDA) to the federal legislature, which takes a risk-based and calibrated approach to the levels of regulation and governance required for AI, depending on levels of 'impact' involved with different models. In this, the Canadian government hopes to align itself more with the EU (see below). Progress remains slow, however, with the proposed bill still under consideration by the Ottawa Parliament's Standing Committee on Industry, Science, and Technology. It is hoped that the bill will be passed before the last date for the dissolution of the current parliament, due by October 2025.

Europe

As the discussion of Canadian developments suggests, the EU has taken a radically different approach than the US to the Hiroshima process, aiming for a more centralized and top-down framework encapsulated in its AI Act (also known as Regulation (EU) 2024/1689), which entered into force on 1 August 2024. It will be applicable as follows:

- **February 2, 2025**, prohibitions on AI practices that pose unacceptable risks come into force – the Commission held a consultation on AI Act prohibitions and AI system definition that closed on December 11, 2024.

- **August 2025**, governance rules and obligations for general-purpose AI models.
- **After 36 months**, rules for AI systems are embedded into regulated products.
- **August 1, 2026**, all other requirements.

Under the Act, the EU will take a risk-based approach which creates varied obligations for providers and deployers of AI, which will also depend on whether it is a 'system,' demonstrating autonomy and adaptiveness, or a General Purpose AI 'model' (GPAI), which can complete tasks in a range of areas, the context in which it is being used, and on the levels of inherent risk involved. Some categories of potential AI use – such as national security, law enforcement, and non-commercial research and development – are exempt from the act. In the commercial arena, the use of AI in relatively simple tools such as spam filters or chatbots is seen as being either minimal or limited risk and, as a result, will only be lightly regulated. Other more complex and impactful uses for AI, such as employment selection or medical treatment, are seen as high-risk and will be subject to a wider range of requirements. AI systems that might be used to infringe personal rights and freedoms (for example, those designed to manipulate and mislead vulnerable people) are treated as unacceptable risks and are therefore prohibited. Failure to comply with the regulation will lead to firms facing a sliding scale of fines up to €35 million (just over $38 million), or 7 percent of annual global turnover if higher, for involvement in high-risk, prohibited practices. Looking forward, 2025 will bring several key milestones for the implementation of the AI Act, including the market withdrawal of prohibited practices in February and the issue of Codes of Practice in May. By August, as noted in the timelines above, all GPAI models will be required to comply with the act.

Like most other countries, the UK has so far operated without a comprehensive regulatory approach to AI, although a spectrum of pre-existing legislation has touched on some relevant concerns around the protection of data security and privacy. The Sunak government – as a signatory to the G7 Hiroshima Process – indicated that it was committed to providing a new framework based on the Process's Principles. In August 2023, it issued an AI regulation white paper promoting a "pro-innovation" approach to AI that suggested a less tightly defined framework than the EU's. The white paper pointed towards a principles-based approach overall, combined with targeted measures for specific industries and future developments in general-purpose AI. This situation became less clear-cut, however, following the change of government at the country's general election in June 2024. The incoming Labour Party had previously stated that it would introduce a new AI regulation in the UK, but without great detail about what this would entail. Some legal observers expected this to be less flexible than the Conservative Party's approach but also narrower than the EU AI Act, focusing chiefly on the most powerful AI systems and models. At the time of writing, the details of a proposed new regulation have not been revealed, but in the announcement of the broad outlines of its legislative program in July 2024, known as the King's Speech the government did state it would "seek to establish the appropriate legislation to place requirements on those working to develop the most powerful artificial intelligence models." A stronger sense of the government's intended direction is likely to emerge in 2025.

Asia-Pacific

Asia-Pacific currently has the most fragmented approach toward regulating AI, although this is far from unusual for a region of such size and economic, political, and cultural diversity. According to a recent assessment by Sidley, a legal firm, over 16 countries in the region have begun the process of regulating AI. However, this also means that the majority (20+ countries) have not yet started.

China is one of the leaders in AI regulation, having enacted various laws and regulations many aspects of which are being replicated around the world to fit the local context. The Cyber Administration of China (CAC) issued an announcement of algorithm filings on June 12, 2024, as part of the implementation of the Algorithm Recommendation Provisions effective 1 March 2022. These provisions require the filing of algorithms that can influence public opinion or drive social engagement, including those used in online information services. The Generative AI Measures became effective on 15 August 15 2023 and apply to GenAI services offered to the public. The Deep Synthesis Provisions came into effect on 10 January 2023 to standardize the management of new technologies, such as algorithms synthetically generating or altering online content, requiring a "Generated by AI" label to be added to such content. The Ethical Review Measures came into force on December 1, 2023, to address the social and ethical challenges of science, technology, and innovation and set out requirements for ethics review procedures that involve humans or animals and may pose ethical challenges.

A small number of countries also appear to be moving towards a more comprehensive approach, to varying degrees influenced by the EU model. Thailand has followed the European lead strongly; it has published, but not yet passed, draft legislation that includes a Draft Royal Decree that applies the same kind of risk-based approach and risk categories as the EU. Others have not been so direct in their emulation of Europe but have also still exhibited a willingness to take a robust stance on oversight. Vietnam's draft Digital Technology Industry Law, under consultation until early September 2024, proposes a range of financial and regulatory incentives for the deployment of AI while also requiring that digital technology firms operate under close state observation. The Vietnamese regulations will also strictly prohibit activities that use personal data for classification purposes.

South Korea's Act on the Promotion of AI Industry and Framework for Establishing Trustworthy AI, which has been going through the National Assembly since 2024, proposes a looser grip on AI development, using the logic of "allow first, regulate later" but still seeks to place significant reporting obligations on those using "high risk" systems and models that potentially affect citizens' rights or well-being. Australia, too, has signaled its intention to follow the EU's path, publishing "Safe and Responsible AI," a set of proposals on AI regulation. The proposals outline ten mandatory guardrails, including transparency and accountability, for AI being used in "high-risk settings." The settings defined as "high-risk" are not explicitly set out, although general-purpose AI appears to be included. Legislation is expected in spring 2025.

Other states in the region have looked more towards the voluntary or principles-based approach that has emerged so far in the US and was initially favored in the UK. Singapore has been the most wide-ranging, introducing its Model AI Governance Framework for Generative AI in May 2024. The framework, while covering all aspects of AI, is principle-based and non-binding. The Singaporean authorities have also promoted a toolkit known as AI Verify, which allows AI providers and deployers to evaluate their own systems and models against international standards such as ISO 42001. Neighboring Malaysia has developed a set of voluntary National Guidelines on AI Governance and Ethics, published in September 2024, which provide a code of ethics for the safe use of AI, with a particular focus on algorithmic transparency and bias prevention. In Hong Kong, by contrast, the local authorities have left most sectors using AI untouched, although the Financial Services and Treasury Bureau (FSTB) issued a set of non-mandatory guidelines for the use of AI in the finance industry in October 2024. This was several months after the Hong Kong Monetary Authority (HKMA) had already announced a forthcoming GenAI Sandbox for the finance industry, looking at the deployment of generative AI in financial services use cases, including fraud detection. In New Zealand, the government has shown a preference for what has been described as "a light-touch, proportionate and risk-based approach to AI regulation," outlined in a cabinet paper issued in July 2024. While New Zealand will amend existing laws to tackle AI-specific problems, it currently has no intention of creating an overarching legislative or regulatory framework.

AI regulatory themes

There obviously continues to be wide surface-level variety in how countries tackle AI regulation. However, it must be stressed again that underneath most of these approaches – whether mandatory or voluntary, principles or risk-based – there is significant commonality in the outcomes that governments wish to see. Governments all share concerns about the following:

- Effectiveness;
- Safety and well-being of individuals;
- Data security and privacy;
- Equity and fairness;
- Oversight and accountability; and
- Channels for challenge and redress.

Alongside these desired outcomes, the most important additions are the need for transparency and explainability. If AI is entrusted with making or enabling important and potentially impactful decisions, governments accept that this cannot be done without understanding the 'how' and the 'why' behind AI's algorithmic processes. AI cannot be allowed to be a 'black box' that operates of its own accord, with no oversight, any more than a human employee might be. This entails that not only the developers and deployers of AI will need to understand how their system works, but they will also need to be able to explain it – clearly, easily, and credibly – to regulators, customers, and any of those who might be affected by a system's decisions – especially an adverse decision.

Compliance and AI

What are the implications of the movement towards AI regulation for financial crime compliance and risk management? As noted at the start of the chapter, many firms are already using or considering using AI technologies in their tech stacks (and our survey indicates the same – see below). Beyond the need to consider the general regulatory principles that are driving the field, are there specific additional concerns that the compliance sector should consider?

Certainly, the Financial Action Task Force (FATF), the international standard-setter on financial crime, has taken a positive view of the use of new technologies in AML/CFT, as set out in its San Jose Principles, issued in 2017. In its 2021 paper, Opportunities and Challenges of New Technologies for AML/CFT, the organization took a deeper dive across a range of new technologies, including varieties of AI such as machine learning and natural language processing (NLP). The paper argued that

AI offered the opportunity to improve efficiency and reduce false positives and negatives in various AML/CFT processes,

including ID&V, ongoing CDD, transaction monitoring, name and transaction screening, the implementation of regulatory updates, and standardized compliance reporting. However, the FATF also stressed the need for caution, suggesting that AI-based systems should be integrated into existing approaches and that attention should be paid to the explainability and auditability of results.

In line with the wider attitude towards AI within their respective jurisdictions, several leading financial crime regulators have supported the application of AI in regulatory technology (RegTech). In 2019, HKMA stated its general support for the use of AI for AML/CFT, issuing a set of High-Level Principles, including familiar criteria such as transparency, necessary for its successful deployment. More recently, in September 2024, HKMA issued a further statement of support for the use of AI in transaction monitoring. The Monetary Authority of Singapore (MAS) has also been one of the strongest regulatory supporters of the use of AI in the fight against financial crime, and in November 2023, the institution's Managing Director, Ravi Menon, expressed his interest in the use of AI, including GenAI in the implementation of the country's new financial crime data sharing platform, COSMIC, discussed later in this chapter.

Despite rising levels of regulatory encouragement for the use of AI in RegTech, even innovative regulators are mindful of fundamental risks and have shown a particular concern about ensuring that AI for AML/CTF does not become an impenetrable black box. It is notable that FATF has not made any recent detailed statements on the role of AI in AML/CFT or its regulation, and, like national regulators, seems more comfortable following in the wake of change in AI regulation in general rather than leading the process with specific measures.

Interestingly, the areas where some regulators appear to be showing the most interest in AI in the financial sector is not in the character of its usage but in whether its usage has been declared and, if declared, whether that usage is genuine. In the US, the Securities and Exchange Commission (SEC) now requires publicly traded companies to include potential AI-linked risk factors in annual reports (the 10-K), and according to an analysis of annual filings conducted in June 2024 by legal firm Orrick, nearly 60 percent of the firms on the S&P 500 recorded an AI-related risk, up from 16 percent in the previous reporting period. A further AI issue for regulators is so-called 'AI washing,' where technology providers claim to use AI in their technology but, in reality, do not. While noted as a problem in Europe and Asia-Pacific, the strongest regulatory action so far has been in the US, where the SEC has taken enforcement actions against firms offering 'AI-driven' recruitment and investment services. According to Gary Gensler, the SEC Chair, "We've seen time and again that when new technologies come along, they can create buzz from investors and false claims by those purporting to use those new technologies… AI washing hurts investors."

Prospects for 2025

AI regulation will move forward in 2025, broadly along the lines set out in the Hiroshima Process. There is limited disagreement at an international level about the appropriate principles for the safe and secure use of AI, but still an array of views on what they should mean in practice. Many countries with AI legislation under consideration will inch towards its implementation, although lobbying by some big tech firms might cause impediments. Indeed, for those countries with more fragmented political systems or closer links between business and government, the regulatory change process will be more drawn out.

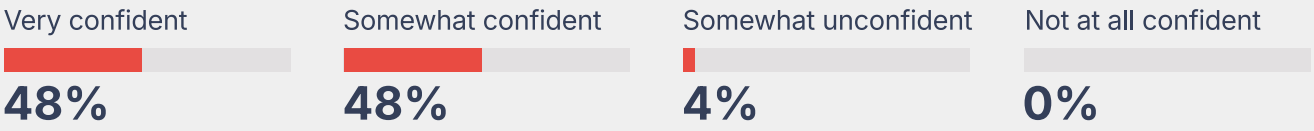
As change proceeds, moreover, there is also likely to be a growing divergence between those countries that seek to take a comprehensive, detailed, and partially mandatory approach to AI regulation and those that prefer narrower, flexible, and voluntary frameworks. It seems likely that, over time, many states with strong trade ties to the EU will align themselves with the bloc's model or at least seek compatibility with it, as many have already done on GDPR and data protection. A smaller group will seek competitive advantage through variation, but they are unlikely to look for the US to provide a template, where the regulatory landscape will remain partial and confused. Based on its campaign rhetoric about preferring AI innovation over regulation, the second Trump administration is likely to encourage this diversity further.

Compliance leaders' perspectives on AI

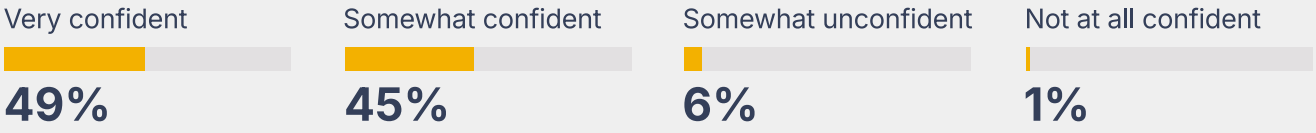
Our survey found high levels of comfort with AI regulatory developments in their jurisdictions, with 70 percent stating that they had a good understanding of what was planned by legislators and regulators in the financial crime compliance space and only 30 percent saying they still had a limited understanding. There was also high confidence amongst respondents that existing or proposed AI regulations would mitigate risks around (a) the need for explainability, (b) deepfake generative-AI-driven frauds, (c) the potential for bias and financial exclusion, and (d) oversight and governance. Confidence was over 90 percent in all cases, apart from risks around bias, although even here, confidence was extremely high.

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

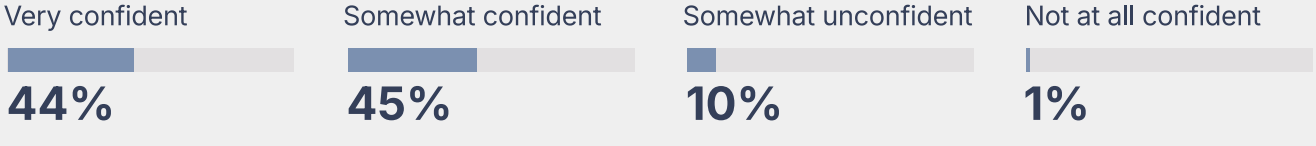
The need to explain financial decisions (e.g. access to a product or service) taken by AI-based solutions



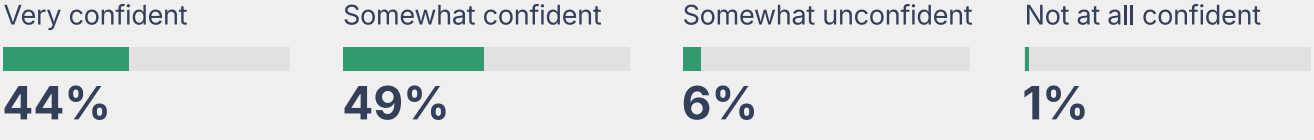
The risk of AI being used to defraud customers in the financial services sector (e.g. through deepfakes)



The risk of algorithms exhibiting an unfair bias towards a particular group of people



The use of AI in financial services without proper governance and standards in place

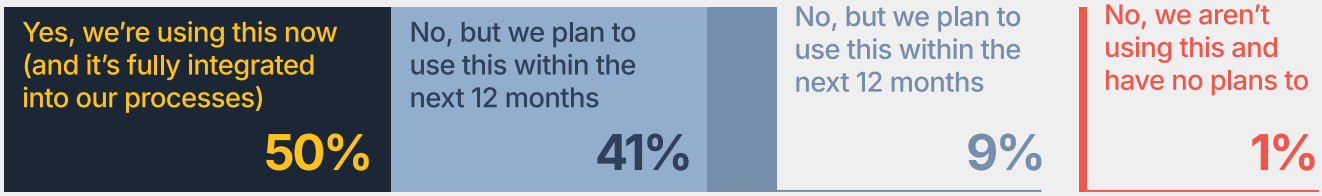


Source: ComplyAdvantage, The State of Financial Crime 2025

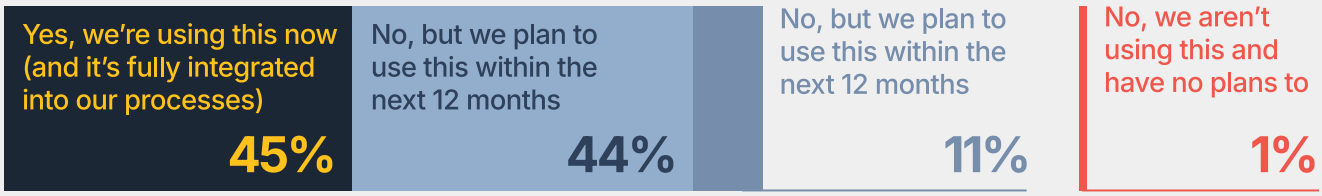
In terms of their own use of AI, our respondents also indicated relatively high levels of deployment for (a) prioritizing transaction monitoring alerts, (b) reducing remediation times, (c) analyzing historical data, (d) forecasting future risks, and (e) producing reporting, such as suspicious transaction reports (STRs). For all five use cases, the proportion of those who said their firms were using AI now, in an integrated way, was in the range of 45-50 percent. The range of those saying that they were using it now, but only in an ad hoc way, was in the range of 41-46 percent. For the remainder who were not using AI at present, most said they were planning to within the next 12 months.

How, if at all, is your organization using or intending to use artificial intelligence within the compliance function?

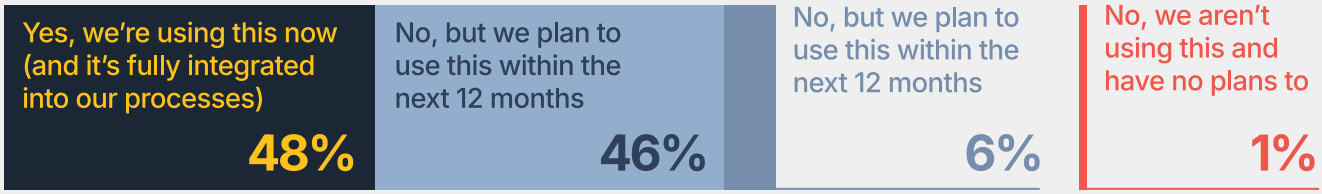
Prioritizing transaction monitoring alerts



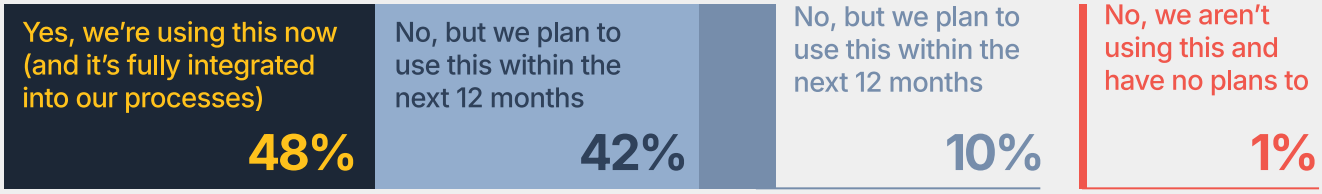
Reducing remediation times



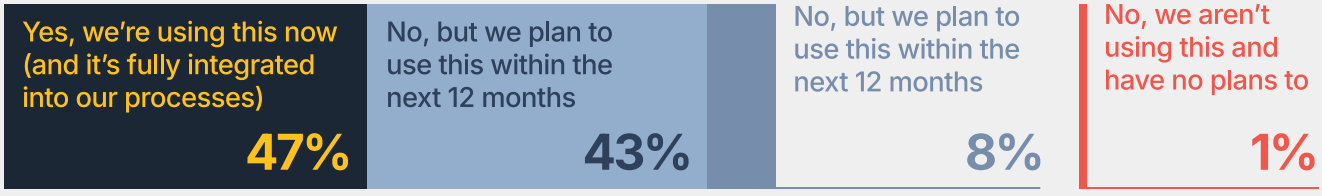
Analyzing historical transaction data



Forecasting future risks or patterns of risk



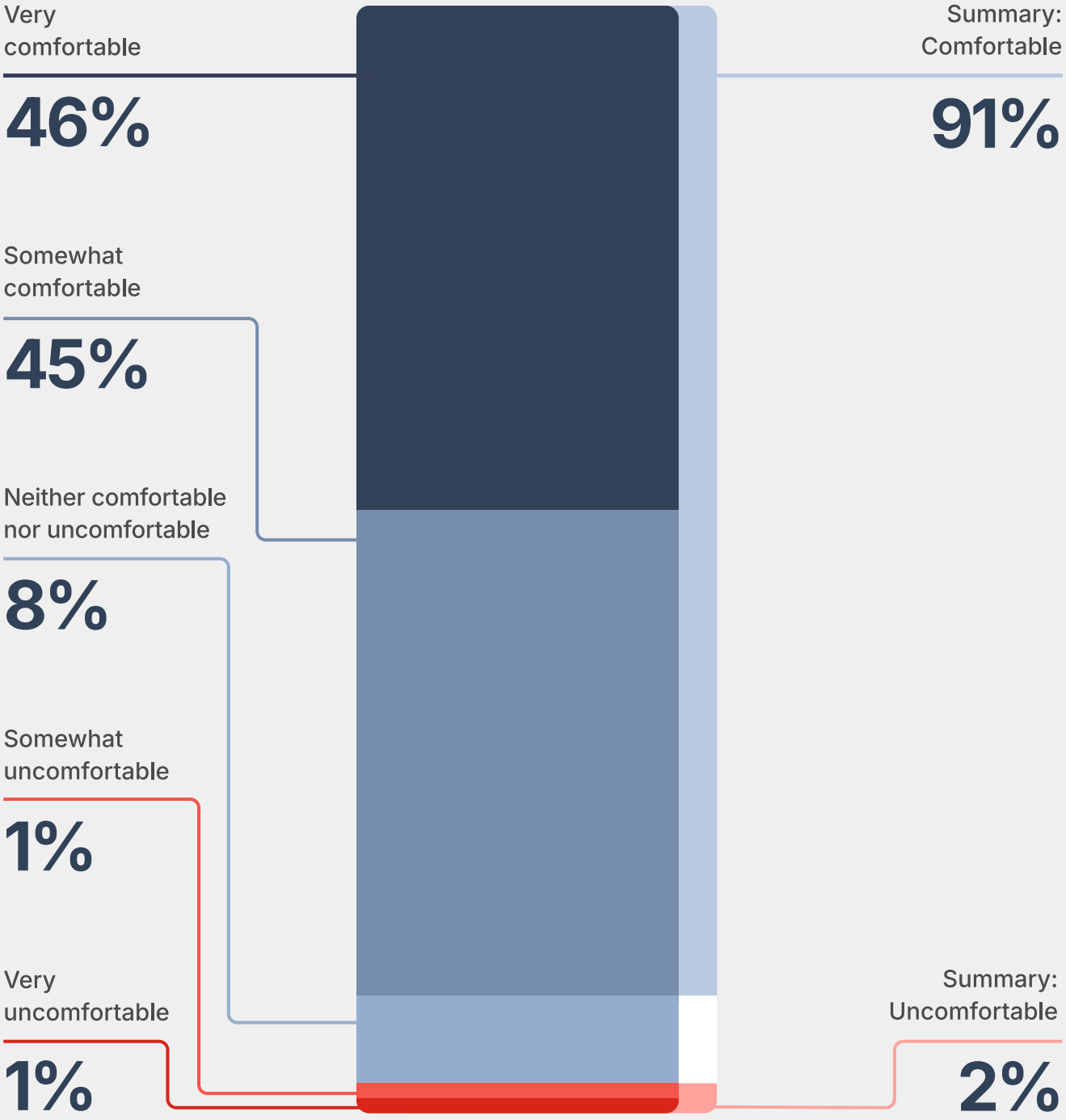
Generating reports (e.g. SARs) using copywriting tools such as ChatGPT



Source: ComplyAdvantage, The State of Financial Crime 2025

Intriguingly – especially in light of respondents' stated understanding of AI regulations and the importance of transparency – significant proportions said they were very comfortable (46 percent) or somewhat comfortable (45 percent) with compromising explainability in return for increased automation and efficiency.

When deploying AI-based compliance solutions, how comfortable are you with compromising explainability in exchange for greater automation and efficiency?



Source: ComplyAdvantage, The State of Financial Crime 2025

What does this mean for me?

- The broad development of the regulatory space for AI, despite divergences, gives your team a lot of guidance on how to deploy systems safely, securely, and in a way that will prove compliant with legal and regulatory demands, even if they continue to evolve in the medium term. The emergence of respected industry standards such as ISO 42001, which aligns with the Hiroshima Process, is helpful. Your organization would be well advised to adopt the ISO standard proactively and seek to work with vendors that have done the same.

- Even while regulatory approaches vary between the 'strong' and the 'soft,' if your organization has an international footprint, it will need to give serious consideration to how it ensures compliance with the toughest regimes, especially the EU AI Act. If you're in North America and Asia-Pacific, you will need to assess whether it might be safer to apply the European 'gold standard' proactively rather than hoping that your own national standards will be accepted in the EU. Past history of trade negotiations between non-EU states and the EU suggests that the Union is unlikely to be flexible on this issue.

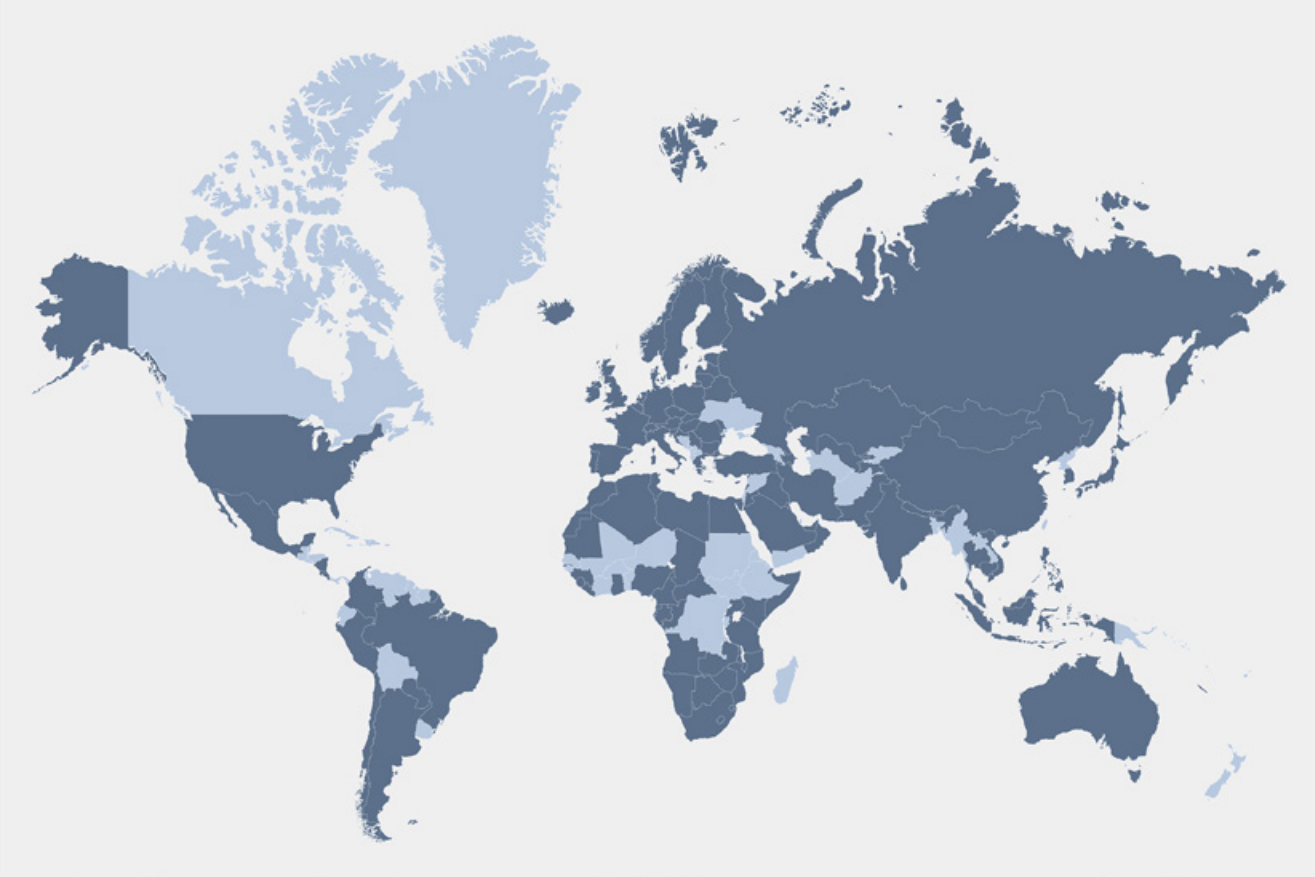
- You also need to take the issues of explainability and auditability extremely seriously – for many teams, more seriously than you are today. Regulators use AI for supervisory purposes: for example, the FCA's **Advanced Analytics Unit** uses AI to help protect consumers and markets. Regulators know the challenges of AI well and are unlikely to be sympathetic if your approach is too lax. Even if regulators' fines remain low relative to turnover – no certainty – the reputational fallout from AI malpractice could be devastating. You therefore need to check again to ensure your AI systems meet the same explainability and audit standards as any other aspect of your compliance function. Taking an 'explainability-first' approach from the outset will minimize remedial work or regulatory risks down the line.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

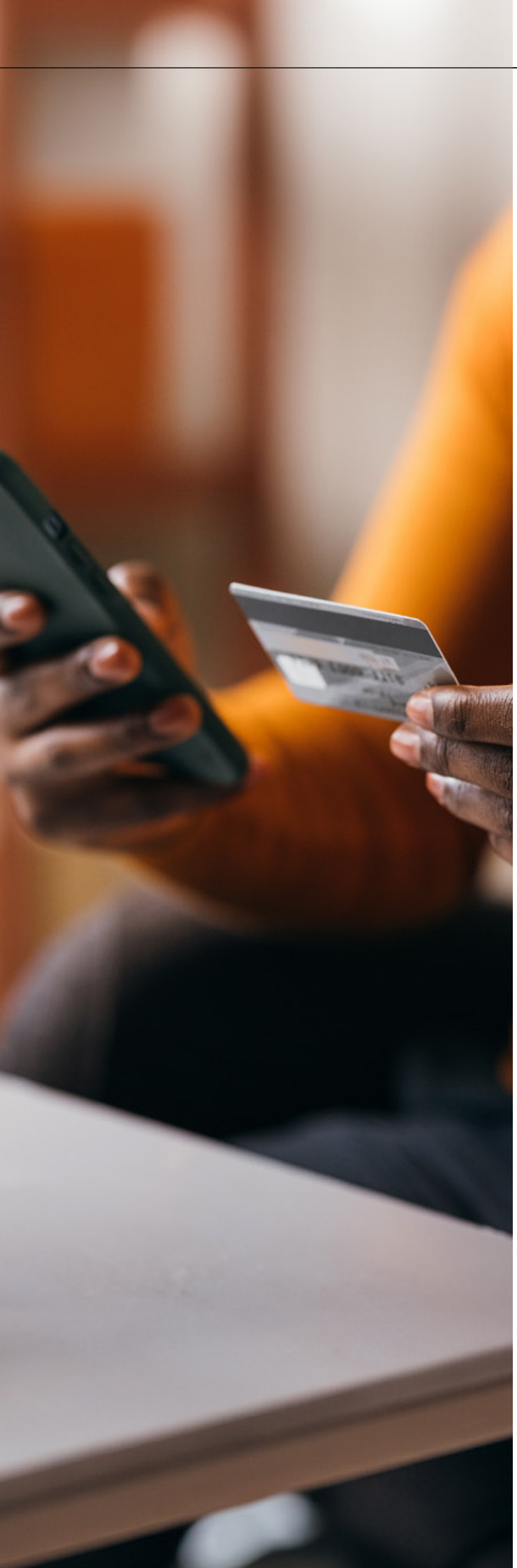
Real-time payment schemes (RTPS)

Real-time payment schemes (RTPS), also known as Fast Payments Schemes (FPS), are among the most positive developments in the financial services sector in the last forty years. They are enabling higher volumes of financial activity and increasing levels of flexibility and financial inclusion, especially for small and medium-sized businesses and retail customers. As the World Bank's Project FASTT (Frictionless, Affordable, Safe, Timely Transactions) has found, RTPS have been deployed across the globe during this century, with a majority of countries taking advantage of the opportunities (see map below, from the World Bank Project FASTT Global Tracker). As of October 24, around 120 jurisdictions have a live system, with many more planning to do so.

World Bank research indicates that in most countries, RTPS usually begins with person-to-person (P2P) payments before moving on to other types of high-volume transaction, such as person-to-business (P2B), which can be trickier to establish because of the need for a 'critical mass' of payment service providers (PSPs) to get involved. However, once this is achieved, system usage tends to grow rapidly, attracting the involvement of other players and encouraging customer demand. As a result, the growth in volume and market size for fast payments has exploded in recent years, with the World Bank estimating that the global RTPS market will grow at a compound annual rate of 35.5 percent between 2023 and 2030, with Asia-Pacific dominating that growth.



Source: World Bank Project FASTT Tracker



Payments and real-time payments

Until relatively recently, domestic payments in most countries were settled by Real-Time Gross Settlement Systems (RTGS) or by an Automated Clearing House (ACH) operated by the central bank, payments regulators, or consortia of financial institutions. In the first instance, large payments between businesses and institutions are settled in real-time. In the second, smaller payments are batched up and settled periodically, on a schedule, and typically overnight. However, with the development of communications and information technology, it has become possible to process domestic payments of any size speedily and securely. RTPS take advantage of these developments, allowing near-immediate account-to-account transfers and funds availability at any time.

Drivers: Technology & standards

In some instances, RTPS operate through augmented versions of existing wholesale payment systems. However, countries are also developing new, dedicated structures to support fast payments, leveraging API standards to bring easy interaction between the diverse in-house systems of PSPs and financial institutions and the potential of distributed cloud computing to enable transaction volumes at scale.

A further essential enabler of RTPS has been the ISO 20022 data standard on messaging between financial institutions, first introduced in 2004. Prior to the standard's introduction, the information in payment messaging between financial institutions – while featuring some common categories such as originator, beneficiary, etc. – was often structured differently, creating unnecessary obstacles to the smooth execution of payments. What ISO 20022 has achieved has been to replace this complex and messy diversity with an agreed range of necessary payment information, structure, and standardized data inputs for any payment message. As we have noted previously, ISO 20022 has helped create a "shared second language" between the parties in financial transactions, which eliminates the need for costly and time-consuming translation, with obvious implications for improving payment speed. So useful has ISO 20022 proven, SWIFT – the Society for Worldwide Interbank Financial Telecommunications – has estimated that by 2025, 80 percent of clearing and high-value payments will be executed according to the ISO20022 standard.

Recent developments

Following the period of rapid growth in RTPS adoption during the last decade, the introduction of new programs has slowed in recent years, although there have been some notable developments across existing schemes:

- **Scheme kick-starts:** Several attempts have been made to replace pre-existing schemes that originally faced limited take-up. South Africa, for example, was one of the pioneers of RTPS, introducing its Real-Time Clearing (RTC) system in 2006, but the scheme had limited market impact. After consultation, the South African Reserve Bank launched a new system, PayShap, in March 2023, specifically designed to support instant mobile-based payments. Similarly, in the US, the Federal Reserve responded to the weak adoption of the Real-Time Payment (RTP) system, introduced in 2017, with the launch of a new instant payment service called FedNow in July 2023. This time, takeup appears to be stronger, with the Federal Reserve reporting that more than 900 financial institutions were offering FedNow by August 2024, up from 35 at the scheme's outset.

- **Scheme upgrades:** In other cases, countries with older, successful systems have been looking to build upon them with new infrastructure. In Canada, its payments regulator, Payments Canada, has been developing a new fast digital payments system called Real-Time Rail (RTR), due for testing by 2026, with the cooperation of Interac, which introduced Canada's first e-transfer system in 2002. In the UK, Pay.UK is working on a New Payment Architecture (NPA), which aims to integrate multiple payment rails, including the Faster Payment System (FPS). The NPA is due to go live in its initial form in 2026.

- **Scheme augmentations:** In some more recent schemes, there are indications of fluid and rapid development. Brazil's Pix, introduced in November 2020, has grown rapidly, with the Banco Central do Brasil (BCB) reporting over 150 million users, mostly businesses. BCB has plans to extend the system's coverage to include recurring payments (Pix Automático) in July 2025, with future developments likely to include Pix Garantido and Pix Credit to support Buy Now Pay Later (BNPL) schemes and the use of Pix infrastructure to enable payments in Brazil's planned Central Bank Digital Currency (CDBC), Drex, due for launch in early 2025.

In the last few years, in fact, the most significant and exciting developments around RTPS are cross-border rather than domestic. Historically, cross-border payments have been cumbersome processes that require relationships between nationally focussed financial institutions and banks with more global coverage, called correspondent banking relationships. In these relationships, the smaller financial institutions rely on international banks as a financial courier service, ensuring the money gets to the desired location and account through their global connections. Obviously, such a complex system was at risk of collapsing into confusion. As a result, a cooperative of banks created the SWIFT electronic messaging system in 1973, which ensured that accurate payment information was routed to the right destination.

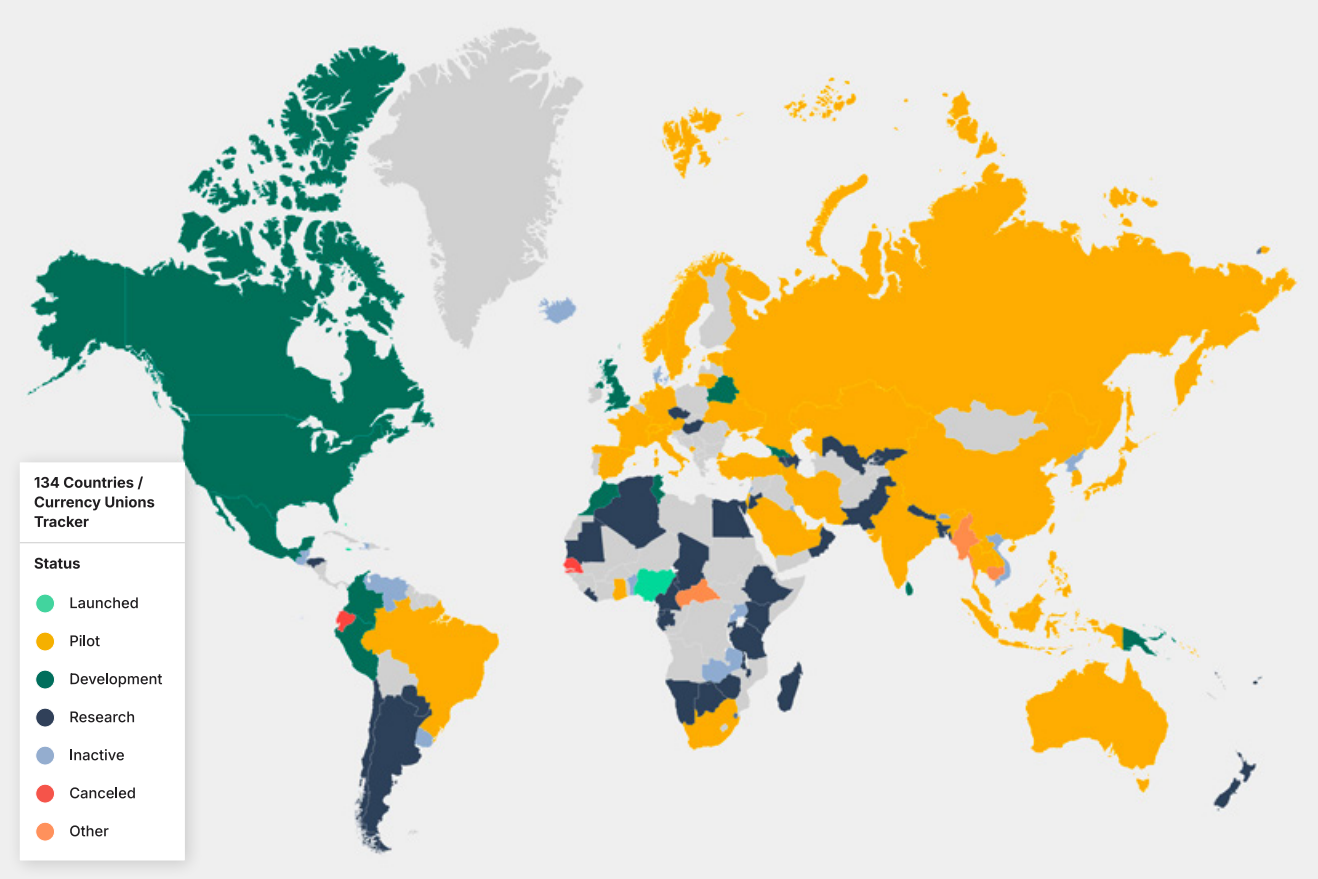
However, in the last decade, developments in financial technology (FinTech) have made this older system look clunky and obsolete.

Cryptocurrencies based on blockchain technology are, in essence, already 'global,' making it possible, in theory, to transact or buy a product or service in any country that allows crypto usage. No long chain of intermediary transactions is necessary, and the execution of payments can be near-immediate.

Nonetheless, cryptocurrencies have not yet taken over as forms of de facto global currency. They are still more likely to be used to transmit value alone rather than for a wider range of real-world purchases. In an attempt to tap into the flexibility of crypto while also providing the trust and stability necessary to ensure wide usage, policymakers have also begun to explore the role of central bank digital currencies (CDBCs), forms of digital currency issued by a central bank with a fixed value, equivalent to the national fiat currency. In 2018, the Bank of International Settlements (BIS) – the central banks' central bank – issued a report noting that while CBDCs could increase the efficiency of domestic payments, their greatest potential would be as an enabler of international payments, with digitalization and links between national central banks allowing payments to be executed quickly, and without the current pattern of 'pass the parcel' between various commercial financial institutions.

There has been considerable excitement about the emergence and potential of CBDCs, especially amongst central bankers, officials, and the officers of legacy financial institutions, seeing them as a way to bring the agility and speed of cryptocurrencies without the feared risk of misuse and volatility.

According to the CBDC tracker, hosted by the think tank the Atlantic Council, of the 134 countries where information is available, 108 are at some point between research on the use of CBDCs through to implementation. So far, however, only three relatively small CBDCs are currently live – those of the Bahamas, Jamaica, and Nigeria – while the digital version of the most significant global currencies – the US dollar, the euro, the Yen, Sterling, or Renminbi – are either in pilot, development, or research. Moreover, given the dollar's international ubiquity, the US Federal Reserve – arguably the most significant stakeholder in the future of CBDCs – remains undecided about whether it will implement a digital US dollar. However, the arrival of the avowedly pro-crypto Trump administration in 2025 might well push the Fed to proceed.



Source: Atlantic Council CBDC Tracker, as of September 2024

Modest progress has been made so far with exploiting CBDCs to tackle cross-border payment challenges. According to the Atlantic Council tracker, nine such schemes looking at primarily wholesale (institution-to-institution) transactions have either been piloted and completed, are in development, or are under consideration. Many of these schemes have proven successful as 'proofs of concept,' such as Project Dunbar between Australia, Malaysia, Singapore, and South Africa, Projects Cedar and Ubin+ between Singapore and the Federal Reserve Bank of New York, and Project Mariana between France, Switzerland, and Singapore. 2024 has seen further positive developments in various other schemes:

- **Digital euro**: In June 2024, the European Central Bank (ECB) published its first progress report on preparing for a digital euro, focusing on privacy standards. The preparation stage for the digital euro began in November 2023, and current plans are to consider launching it in October 2025.
- **Project Agora:** In April 2024, BIS announced a new project involving the central banks of France, Switzerland, the UK, Japan, South Korea, Mexico, and the Federal Reserve Bank of New York to explore the use of digital tokens and 'smart contracts' in the execution of international wholesale payments.
- **Venus initiative:** In June 2024, the central banks of France and Luxembourg announced the success of the Venus pilot scheme, launched in November 2022. The scheme used a wholesale CBDC to settle trades in tokenized bonds issued by the European Investment Bank (EIB) on a private blockchain.
- **Project mBridge:** In June 2024, BIS announced that this CBDC collaboration with the central banks of Thailand, UAE, Saudi Arabia, Hong Kong, and China had developed a minimum viable product (MVP). The project is focused on developing the mBridge Ledger, a new blockchain to facilitate multi-bank CBDC transactions between participating central banks and private financial institutions.

However, most completed projects and current studies remain feasibility studies rather than practical schemes, and in nearly all cases, a proof of concept has not yet led to full deployment. Moreover, geopolitical challenges have risked undermining some schemes, especially where involved states have strong financial and economic relations with other states under Western sanctions.

In October 2024, for example, the BIS announced it would be withdrawing from Project mBridge, apparently over the potential for the scheme to become a sanctions evasion 'workaround' for China's close partner, Russia.

However, CDBCs are not the only option being explored by countries looking at rapid cross-border payment schemes. Quick response (QR) codes – two-dimensional matrix barcodes – have been widely deployed to support cross-border retail payments in Southeast Asia, with various bilateral cross-border QR-linkage schemes launched from 2020 onwards. This trend continued in 2024, with the central banks of Thailand and Laos announcing a 'go live' between their two countries in April, with Malaysia and Cambodia following suit in September. More broadly, the international community has been looking at the potential for APIs to act as 'translators' between national RTPS, aiding the development of cross-border payments. In October 2020, the Group of 20 leading economies (G20) endorsed the roadmap developed by the Financial Stability Board (FSB), an international body established by the G20, and the BIS's Committee

on Payments and Market Infrastructures (CPMI), on the potential value of APIs in the development of effective cross-border payments systems.In October 2024, CPMI issued further recommendations and a toolkit for the use of APIs in cross-border payments to the G20, noting the need for greater coordination of API technical standards between countries to ensure their wider usage.

A further significant cross-border scheme, which, despite being relatively long-standing, has seen major recent developments, is the Single Euro Payments Area (SEPA). SEPA credit transfers (bank transfers or wire transfers) were first introduced in 2008, followed by direct debits in 2009. In 2012, a SEPA regulation was adopted by the EU, creating a dedicated legal framework that sets rules and standards under which participating financial institutions must operate. According to these standards, credit transfers are expected to take no more than one business day, and direct debit transfers take one to two days, or at least three days between businesses. SEPA currently consists of 36 members, including all of the EU and several others, such as Norway, Switzerland, and the United Kingdom.

In November 2017, the EU payments regulator, the European Payments Council (EPC), also launched SEPA Instant Credit Transfer (SCT Inst), which required participating financial institutions to complete credit transfers up to an agreed limit (now €100,000, about $105,000) in less than 10 seconds. However, while participation in SCT Inst has not been obligatory, the introduction of a new EU Instant Payments Regulation (IPR), which came into force in April 2024, has created a new mandatory requirement for all PSPs to offer instant payments. According to the schedule set out in the regulation, all PSPs operating in the Eurozone excluding electronic money institutions (EMIs) and payment institutions (PIs), will be required to be able to receive instant payments on 9 January 2025 and send them on 9 October 2025. Obligations will extend to EMIs and PIs, as well as the full range of PSPs outside the Eurozone, throughout 2027. How financial institutions achieve these goals is not prescribed, but what they do is deemed essential.

Prospects for 2025

2025 will be a big-bang year for real-time payments in Europe, and as ever, this is likely to have an ongoing ripple effect on the wider world. Various other streams of regulatory and governmental activity will add to the momentum toward widespread takeup of real-time payments within countries and across borders in 2025. Asia-Pacific will likely remain a leader in using QR code linkage and APIs to create bilateral links supporting growing cross-border retail payments in the region. Based on the past experience of major European projects, the introduction of the digital euro, planned for the autumn of 2025, is likely to slip to 2026. However, its development will need to be watched closely; if successful, it too could have a revolutionary effect. Schemes such as Project mBridge, if used by a wider group of emerging and developing economies, are likely to increase integration between those economies while at the same time risking a growing divide with the developed world, especially if this is overlaid with political tensions between the West and its adversaries.

What does this mean for me?

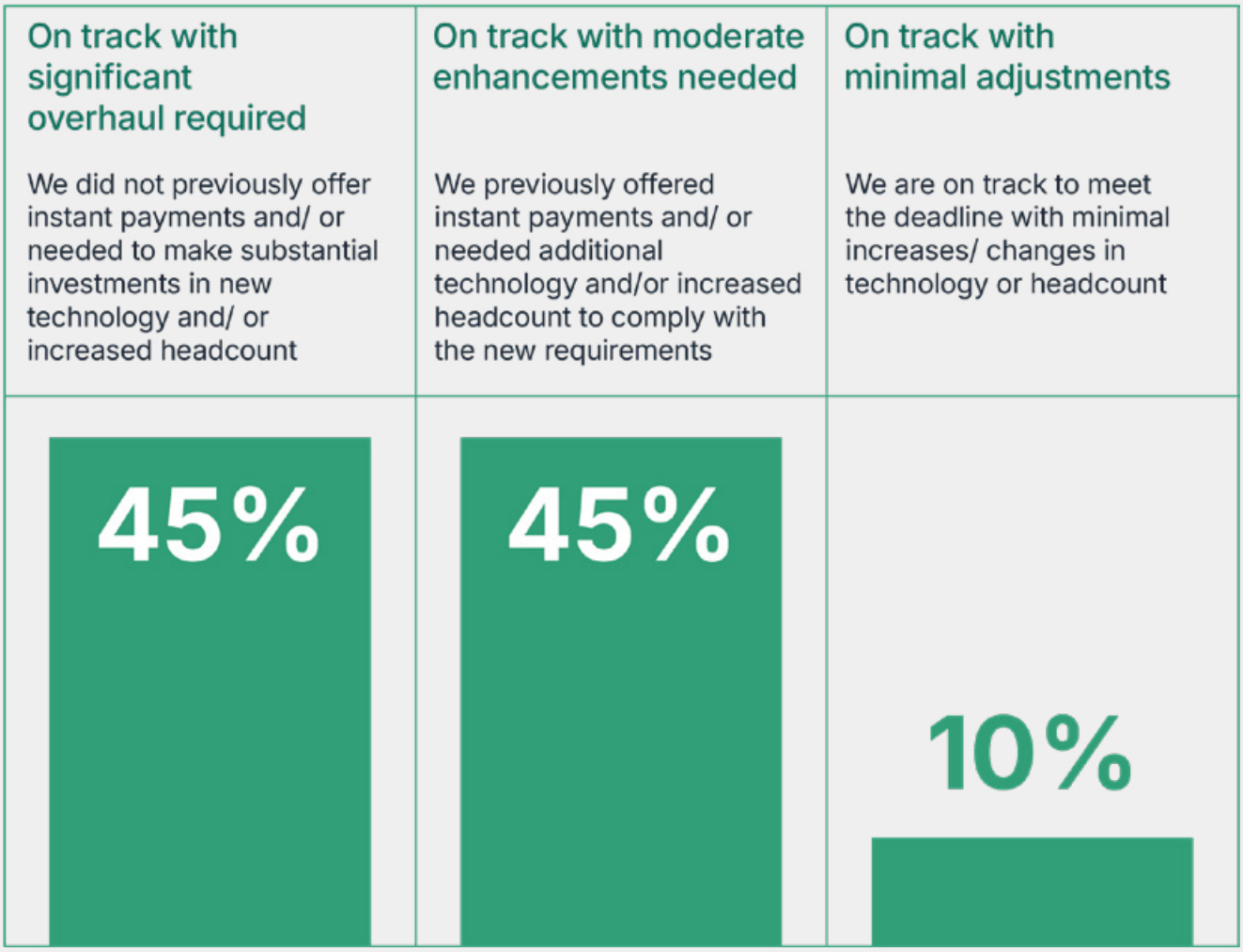
- The development of RTPS, nationally and cross-border, raises serious challenges for PSPs and other financial institutions. Beyond the obvious technical issues, you must ensure that your firm has near real-time screening and monitoring in place to ensure risks are detected and mitigated quickly.
- Two key areas deserve particular consideration: firstly, the preference of fraudsters and other financial criminals for fast payments, which allow them to take and move money quickly, and secondly, widening sanctions list requirements that will put an onus on real-time transaction screening. In the first instance, you risk being at the mercy of large losses from criminals; in the second, from enforcement action, fines, and reputational damage.
- To tackle both issues, your team will need monitoring and payment screening systems that comply with the highest technical standards, especially ISO 20022, and have the flexibility and agility to detect risks quickly and accurately. A world of real-time payments demands real-time risk management.

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

Compliance leaders' perspectives on real-time payments

According to our survey, respondents are taking real-time payment regulations like SEPA extremely seriously and are looking to ensure their tech stacks are prepared to meet more stringent requirements. Of our respondents in Germany, France, and the Netherlands, 41 percent said they required a significant overhaul to meet the IPR but that they were on track to do so despite not previously offering instant payments. 49 percent said they already provided instant payments and only needed to make moderate enhancements to meet the IPR. 10 percent said they would need minimal changes, and no respondents assessed that they were likely to miss the deadline.

How has your organization responded to the January 2025 deadline for receiving instant payments under the SEPA ICT scheme?



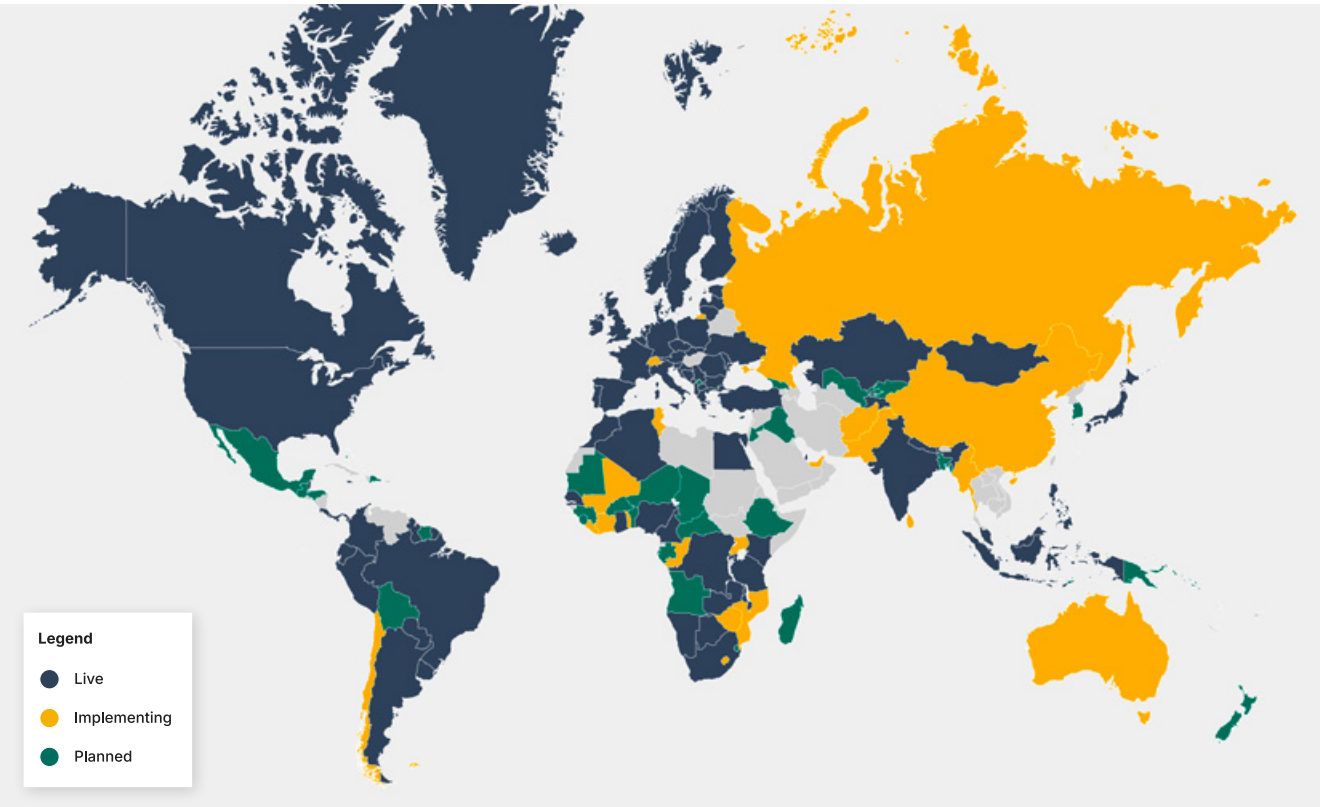
Source: ComplyAdvantage, The State of Financial Crime 2025

Beneficial ownership & corporate transparency

Transparency around the beneficial ownership (BO) and ultimate beneficial ownership (UBO) of companies – those who ultimately own and/or control a given company – has been a major political issue of the last decade.
A succession of public revelations, such as the LuxLeaks in 2014, Panama Papers in 2016, and the Pandora Papers in 2021, have enabled investigative journalists to show how shell companies and trusts with opaque ownership structures and limited transparency requirements have been used by many criminals and corrupt officials to launder illicitly generated funds, skirt or evade tax commitments, and evade sanctions. In response, governments and international groups such as the G7 and G20 have developed shared approaches to BO transparency, with FATF taking a strong lead on the issue. In March 2022, FATF strengthened standards on BO, set out in an updated Recommendation 24. The recommendation required all member states to introduce a public BO register and obliged firms to take a "multi-pronged" approach to collecting BO information from clients, public, and commercial sources. In March 2023, FATF issued updated guidance on taking a risk-based approach to implementing the Recommendation, and in March 2024, it issued further guidance on taking a risk-based approach to the BO of trusts and other similar arrangements.

Global transparency

According to research by Open Ownership, a not-for-profit organization that promotes corporate transparency, 90 countries already have a live BO register, 26 are in the process of implementing a register, and 41 are planning a register, with only a relatively small number of countries concentrated in the Middle East and Southeast Asia currently not taking any relevant action (see map). However, despite the apparently positive global picture, the reality of what this means on the ground can vary.



Source: Open Ownership Map, as of November 2024

Regional developments

This is nowhere more apparent than in North America, where Canada and the US have traveled at very different speeds in increasing transparency. In June 2019, Canada altered its Canada Business Corporations Act (CBCA) to require firms to create an internal register of Individuals with Significant Control (ISC), with ISCs having over 25 percent of shares or voting rights. As of January 2024, businesses must file annual returns to Corporations Canada. A director or officer of a company found responsible for failure to comply can be fined up to $1 million (Canadian – around $717,000 US) and/or imprisoned for up to five years. Some information filed - the names, addresses, and dates of control of the ISCs – will be available to the public, probably in early 2025. Following the conclusion of the Cullen Commission in June 2022, looking at the scale of money laundering in British Columbia (BC), the province is scheduled to extend access to its existing provincial BO register to the public in 2025.

On one level, the US has also made significant progress in recent years. In January 2024, the Corporate Transparency Act (CTA), passed in 2021, came into effect. Under the act, corporations and limited liability companies were required to report their beneficial ownership information (BOI) to FinCEN based on a 25 percent plus standard of ownership and/or control. Companies created or registered before the start of 2024 will have one year to file (a deadline of January 1, 2025), and those created or registered in 2024 or later will have thirty days from their notification of a successful application to register to file. This data will then be kept in FinCEN's Beneficial Ownership Information System (BOIS).

However, access to BOIS will be strictly controlled, with only government agencies, law enforcement, regulators, and financial institutions able to obtain information under specific circumstances related to law enforcement, national security, or the execution of regulatory requirements, such as AML/CFT due diligence. The public will not have visibility, and the available access will be strictly circumscribed. Nor will access be immediate to all stakeholders, with financial institutions the last to receive it. A date for this has not yet been set. Given the slow timescales for implementation so far, it seems likely that if this comes in 2025, it will be towards the end of the year at least.

Further delays might also come from legal challenges. In March 2024, a district judge in Alabama ruled that the CTA and the collection of BOI were unconstitutional in response to a case from the National Small Business United (NSBU). The US Treasury subsequently appealed the decision, and the US Court of Appeals for the Eleventh Circuit heard the case in September 2024 with no judgment provided. While most legal observers believe that this case will eventually fail, the prospect of further legal challenges in other states raises questions about the long-term prospects for the legislation, especially with the return of an anti-regulatory Trump administration in January 2025.

Across the Atlantic, transparency's fortunes have also been mixed. The UK has been a relatively good news story, although far from perfect; a publicly accessible registry of Persons of Significant Control (PSC) has been in existence since 2016, and a Registry of Overseas Entities (POE) with interests in UK land and property since 2022. However, critics have questioned the completeness and integrity of both. In response, the Economic Crime and Corporate Transparency Act 2023 (ECCTA) has sought to strengthen the regime further. Several of its key provisions already came into effect in 2024. Companies House, the existing business registrar, will have its powers of investigation and punishment enhanced. As of autumn 2024, this includes a new framework for imposing financial penalties on those that do not comply with transparency requirements, and throughout 2025, it will expand to include the right to expedite the striking off of companies, carry out checks on authorized corporate service providers (ACSPs). It will eventually require PSCs and directors to verify their identities on incorporation or during annual filings. However, when this last change will be implemented is far from certain, as it will require considerable changes to Companies House technology and processes.

In the EU, however, the cause of BO transparency has faced significant difficulties. At least initially, the EU was a leader in the field. Under the EU's AML/CFT regulations, in particular Anti-Money Laundering Directives (AMLDs) Four and Five, member states have been required to ensure that:

- Businesses incorporated within their jurisdiction hold up-to-date and accurate BO information;
- That this information be held in a central registry accessible to competent authorities, AML/CFT regulated firms, and that
- According to AMLD5, the material should be accessible to members of the public regardless of their intent.

Nonetheless, as the work of advocacy groups such as Transparency International (TI) demonstrated, the effective implementation of these changes at the national level was varied in practice, with many countries dragging their feet on free public access. Matters became even more problematic in November 2022, moreover, when the Court of Justice of the European Union (CJEU) invalidated the right to public access, holding that an unrestricted right infringed privacy and data protection rights and that "legitimate interest" did indeed need to be demonstrated. Within weeks of the ruling, various states suspended their registers or removed rights of public access, and a year after the ruling, TI found that in 13 of 27 member states, journalists and civil society groups with legitimate cause could either not gain access, or faced significant hurdles in doing so.

EU authorities have sought to remedy this conflicted situation as part of its AML/CFT reform package, which was finalized in June 2024. As part of a new Sixth AMLD, the EU has decided that full public access should not be allowed, with the criteria of 'legitimate interest' applied instead. However, the term "persons of legitimate interest" has been given more specificity to include those working in the media, civil society organizations, and higher education. Member states will be required to implement the requirements of the new AMLD by July 10, 2027, suggesting that it will take several more years before there is a truly consistent approach across the EU.

Finally, progress towards transparency in the Asia Pacific has been relatively slow, and where BOs are available, access tends to be relatively restricted. In Singapore, for example, the Register of Registrable Controllers (RORC), maintained by the Accounting and Corporate Regulatory Authority (ACRA), is only open to public authorities and law enforcement.

In countries that do not already have BO registers, progress has remained relatively sluggish in 2024. In April, for example, the Companies Commission of Malaysia (CCM) introduced new guidelines for BO information, which tightened time requirements for lodging BO information with the CCM.

Nonetheless, access to data held at the company level or by the CCM is limited to public authorities and AML/CFT-obliged institutions.

In Australia, according to Open Ownership, the government has committed to introducing a publicly available registry, but timescales are vague, with 2025 the date for implementation. Meanwhile, despite a stated intention to create a public BO register in New Zealand, TI reported in September 2024 that the government had suspended its plans because of concerns about compliance burdens on businesses. In the Asia-Pacific region, the cause of corporate transparency is a long distance to travel.

Prospects for 2025

The push towards corporate transparency has been one of the most familiar and welcome aspects of the financial crime landscape over the last decade. Governments of all political complexions and from all regions, encouraged by civil society groups and investigative journalism, have expressed their support for more openness. This said, however, the practical realities of BO transparency have been much less impressive so far, with even champions of information accessibility, such as the EU, struggling to make changes permanent in the face of various challenges from businesses and individuals. Indeed, there is a sense that the pro-transparency tide might now be on the turn, at least for now. Official support for more corporate transparency in the US is almost certain to dissipate under the Trump administration, and if anything, it seems likelier that it will seek to interpret rights of access under the CTA extremely narrowly. While it is far too soon to say that the age of corporate transparency is over, the cause is likely to face a much less welcoming political environment.

What does this mean for me?

- Regulated businesses have long hoped that BO registries would be a major help in the conduct of CDD, and indeed, campaigners have suggested that they would be a major tool in the fight against economic and financial crime. Nonetheless, the current political and regulatory trends around BO tend to suggest that state managed registries will not prove to be a solution to the problem of corporate opacity.

- At the same time, your firm is still obligated to identify the BO of its clients under AML/CFT legislation. This requires, as FATF suggests, a "multi-pronged" approach that uses varieties of public information, along with commercial data, to build a full picture and identify discrepancies and risks. You need to ensure, therefore, that your firm engages with vendors that can offer credible and comprehensive data that will support your CDD, monitoring, and screening processes.

Andrew Davies
Global Head of Regulatory Affairs, ComplyAdvantage

Public-private partnerships

Since 2015, a growing number of countries in Europe, the Americas, Africa, and Asia-Pacific have created public-private partnerships (PPPs) aimed at improving information and knowledge sharing on financial and economic crime between the sectors. These partnerships have developed to cover specific financial crime risks, such as terrorist financing and human trafficking, to more comprehensive arrangements looking at a full spectrum of financial and predicate crimes. Many operate at a strategic level, focusing on sharing thematic risks and typologies, while a smaller number have looked to share operational and tactical intelligence to enable and aid specific law enforcement operations. These initiatives have been broadly welcomed across both the public and private sectors, with FATF providing strong support and guidance on their implementation.

Nonetheless, the rapid growth in numbers and varieties of schemes appears to have slowed after an initial burst; instead, 2024 has been less a year of geographic expansion and more of evolution within existing frameworks. One of the first PPPs was the UK's Joint Money Laundering Intelligence Taskforce (JMLIT), which was created in 2015. Under the previous UK government's Second Economic Crime Plan (2023-2026), the next steps for PPPs included expanding the existing model to "take a truly multi-stakeholder approach." An example of this was revealed in July 2024, when the National Crime Agency (NCA) announced that it was working with seven UK banks in a pilot scheme to share account data "indicative of potential criminality," with a particular focus on tackling organized crime. As part of the scheme, which ran until October 2024, staff from the NCA and the participating banks worked together in a joint team to identify risks.

Other positive developments included the launch of MAS's COSMIC platform in April 2024, which turned legal changes to enable private sector information-sharing made in 2023 into concrete reality. COSMIC (Collaborative Sharing of Money Laundering/TF Information & Cases) is a centralized digital platform to enable information sharing on financial and economic crimes between financial institutions, developed by MAS and six major banks. Via COSMIC, the six participating financial institutions will be able to share customer information with their partners when data in a customer profile or transactional behavior matches a number of indicators of suspicion. Initially, the scheme will remain voluntary and limited to the six founder banks and will focus on three key risk use cases, including the misuse of legal corporate persons (i.e., shell companies), trade-based money laundering (TBML), and proliferation financing. If judged to be successful, MAS has said it will consider extending the scheme to a wider range of risk types and member institutions in the financial industry and other regulated sectors.

In Canada, Bill C-69 amended section 11.01 on disclosure without consent in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) to allow private-to-private information sharing. This allows firms to share personal information if "reasonable" to detect or deter money laundering, terrorist financing, or evasion of sanctions; notifying the individual would compromise the ability to deter or detect criminal activity and if the disclosure is made in line with regulations. Reporting entities have been given immunity when disclosing or collecting information in good faith. Privacy protections are kept in place for personal information, and the Office of the Privacy Commissioner has an oversight role.

Hong Kong also has a strong track record of public-private partnerships, with HK$1.1 billion restrained or confiscated since the inception of the Fraud and Money Laundering Intelligence Taskforce (FMLIT) and HK$12.3 billion intercepted by the 24/7 stop-payment mechanism established by banks and the Police's Anti-Deception Coordination Centre. On September 30, 2024, the Hong Kong Monetary Authority released the consultation conclusions on information sharing among authorized institutions to aid in the prevention or detection of crime, summarizing views from the banking sector and the public on sharing information on customer accounts amongst authorized institutions to prevent and detect crime. Hong Kong will amend the banking ordinance to reflect support for private-to-private information sharing, which will be passed before the legislative council in 2025.

One small setback has occurred, however, in one of the most advanced and innovative PPPs. Since 2021, a group of five major Dutch banks have worked with the authorities on developing Transaction Monitoring Netherlands (TNML), a joint project for collective transaction monitoring focused initially on commercial banking. Indications from the project had been positive, suggesting a reduction in false positive 'noise' from alerts and identifying an increasing number of previously unknown risks. Unfortunately, the finalization of the EU's reform AML reform package in the summer of 2024 led the main stakeholders to conclude that they would need to re-evaluate the scheme in the light of new private-to-private sector information-sharing requirements set out in the AML Regulation (AMLR). According to the regulation, private sector institutions should only be able to share information related to specific and identified suspicious transactions rather than more general concerns about clients or groups of clients. TMNL has said that although it hopes to revise its model in response, it does not expect to begin operating again until mid-2027.

Prospects for 2025

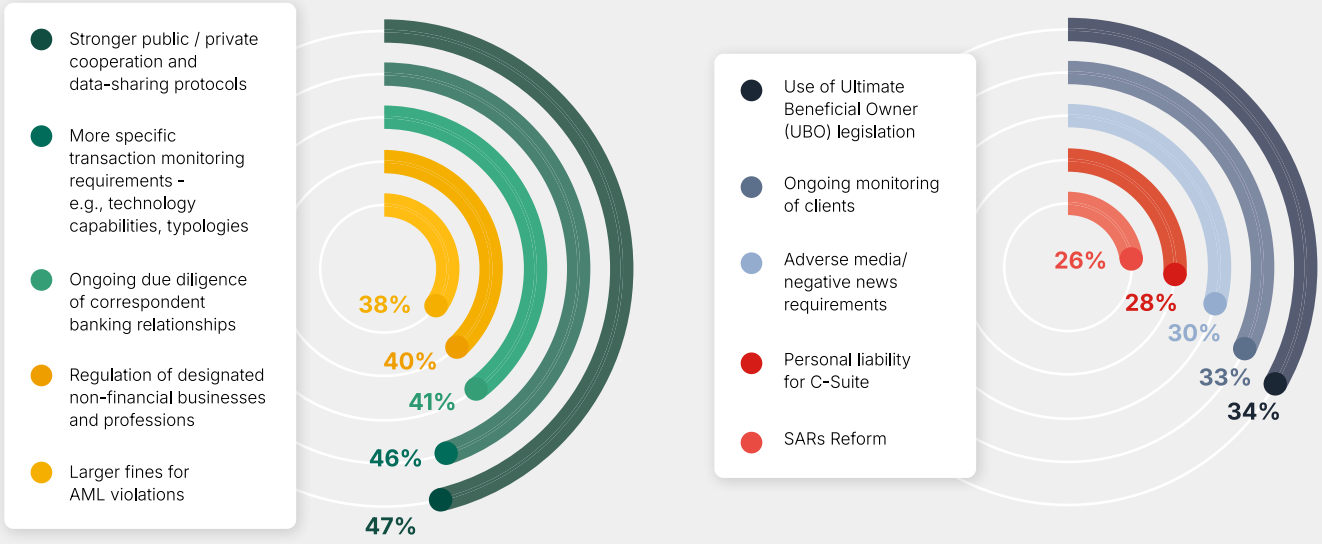
The push towards corporate transparency has been one of the most familiar and welcome aspects of the financial crime landscape over the last decade. Governments of all political complexions and from all regions, encouraged by civil society groups and investigative journalism, have expressed their support for more openness. This said, however, the practical realities of BO transparency have been much less impressive so far, with even champions of information accessibility, such as the EU, struggling to make changes permanent in the face of various challenges from businesses and individuals. Indeed, there is a sense that the pro-transparency tide might now be on the turn, at least for now. Official support for more corporate transparency in the US is almost certain to dissipate under the Trump administration, and if anything, it seems likelier that it will seek to interpret rights of access under the CTA extremely narrowly. While it is far too soon to say that the age of corporate transparency is over, the cause is likely to face a much less welcoming political environment.

Compliance leaders' perspectives on information sharing

In our survey, respondents were asked where the tightening of AML regulation would have the greatest impact on the fight against financial crime. The lead category was stronger public-private cooperation and data-sharing protocols (47 percent), followed by the closely related issue of guidance on transaction monitoring requirements and typologies (46 percent).

Firms are clearly looking to FIUs, law enforcement, and regulators for better support and guidance than they feel they are currently receiving. Lower down the ranking, in sixth position, was the tightening of UBO legislation (34 percent), again suggesting that firms are looking for official support to aid their fight against financial crime. Having the right data and information is vital.

Which area 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 2025

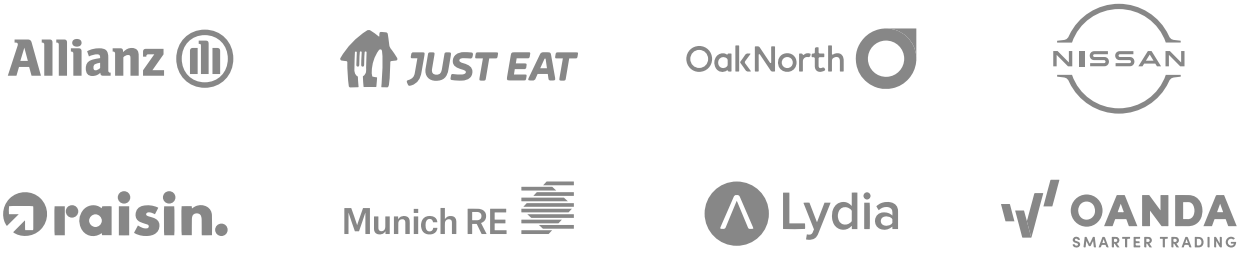
- Our survey suggests that regulated firms are eager to have the right information and guidance to identify and mitigate financial crime risks. There is no desire to pass responsibility to the public sector, but certainly an appetite for a much closer and more trusting working relationship with them.
- Over the last decade, the atmosphere around such cooperation has been extremely positive, and there has been something of a 'boom' in the number of PPPs since 2015. There have also been examples of public and private stakeholders in some jurisdictions seeking to push the boundaries of collaboration further and faster than the majority. These have acted as role models for many others.
- Nonetheless, PPPs have only been able to go so far and, in most cases, still involve only the largest financial institutions. Even though the support and guidance they provide to the private sector has provided a boost to AML/CFT efforts, they have not been game-changers in most countries for most firms.
- This indicates that while businesses should seek to be as involved as possible in PPPs, leveraging information for government agencies to better manage screening, monitoring, and ongoing due diligence, they also need to combine this with an in-house approach that takes full responsibility for gathering the best risk data possible, and using the most agile and flexible platforms.

About ComplyAdvantage

ComplyAdvantage is the financial industry's leading source of AI-driven financial crime risk data and detection technology. ComplyAdvantage's mission is to neutralize the risk of money laundering, terrorist financing, corruption, and other financial crime. More than 1000 enterprises in 75 countries rely on ComplyAdvantage to understand the risk of who they're doing business with through the world's only global, real-time database of people and companies. The company actively identifies tens of thousands of risk events from millions of structured and unstructured data points every single day. ComplyAdvantage has four global hubs located in New York, London, Singapore and Cluj-Napoca and is backed by Ontario Teachers', Index Ventures and Balderton Capital. Learn more 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 2025 is based on a survey of 600 C-suite and senior compliance decision-makers across the US, Canada, UK, France, Germany, Netherlands, Singapore, Hong Kong, and Australia.

All respondents currently work in financial services and fintech organizations, primarily in banking and payments, with 50+ employees and at least $50m in revenue.

COMPLY ADVANTAGE®

complyadvantage.com

2025