



The State of Financial Crime **2024**

Contents

01.



Spotlight on Financial Crime

The rising cost of compliance and the need for highly skilled teams	05
Innovations in the payments landscape	07
The rise of AI and the convergence of cybercrime & money laundering	10
Bribery, corruption, and PEPs	14
Regional Trends	18
▸ The Americas	18
▸ Europe	22
▸ Asia	24
▸ Middle East & Africa	26

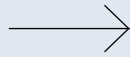
02.



Geopolitics and Sanctions

What are Sanctions?	30
Major Hotspots	31
▸ Russia	31
▸ Iran	43
▸ North Korea	46
▸ China	49
Regional and Thematic Review	56
▸ Europe	56
▸ Middle East	57
▸ Asia-Pacific	57
▸ Africa	58
▸ Latin America	59
▸ Terrorism	60
▸ Organized Crime	61
2024 Prospects	61

03.



Regional Regulatory Trends

Global AML/CFT Developments	66
Crypto Asset Digital Framework	68
The United States	70
Canada	74
The EU, France, and Germany	76
The United Kingdom	81
China	83
Singapore	84
Australia	86
Indonesia	88
Latin America and the Caribbean	89
Africa and the Middle East	90

04.



Regulatory Themes

Artificial Intelligence	93
Real-Time Payment Schemes	96
Beneficial Ownership and Corporate Transparency	98
Continued Growth of Public-Private Partnerships	100
Circumventing Sanctions	102

[↑](#) Back to beginning

[→](#) Next section

Spotlight on Financial Crime



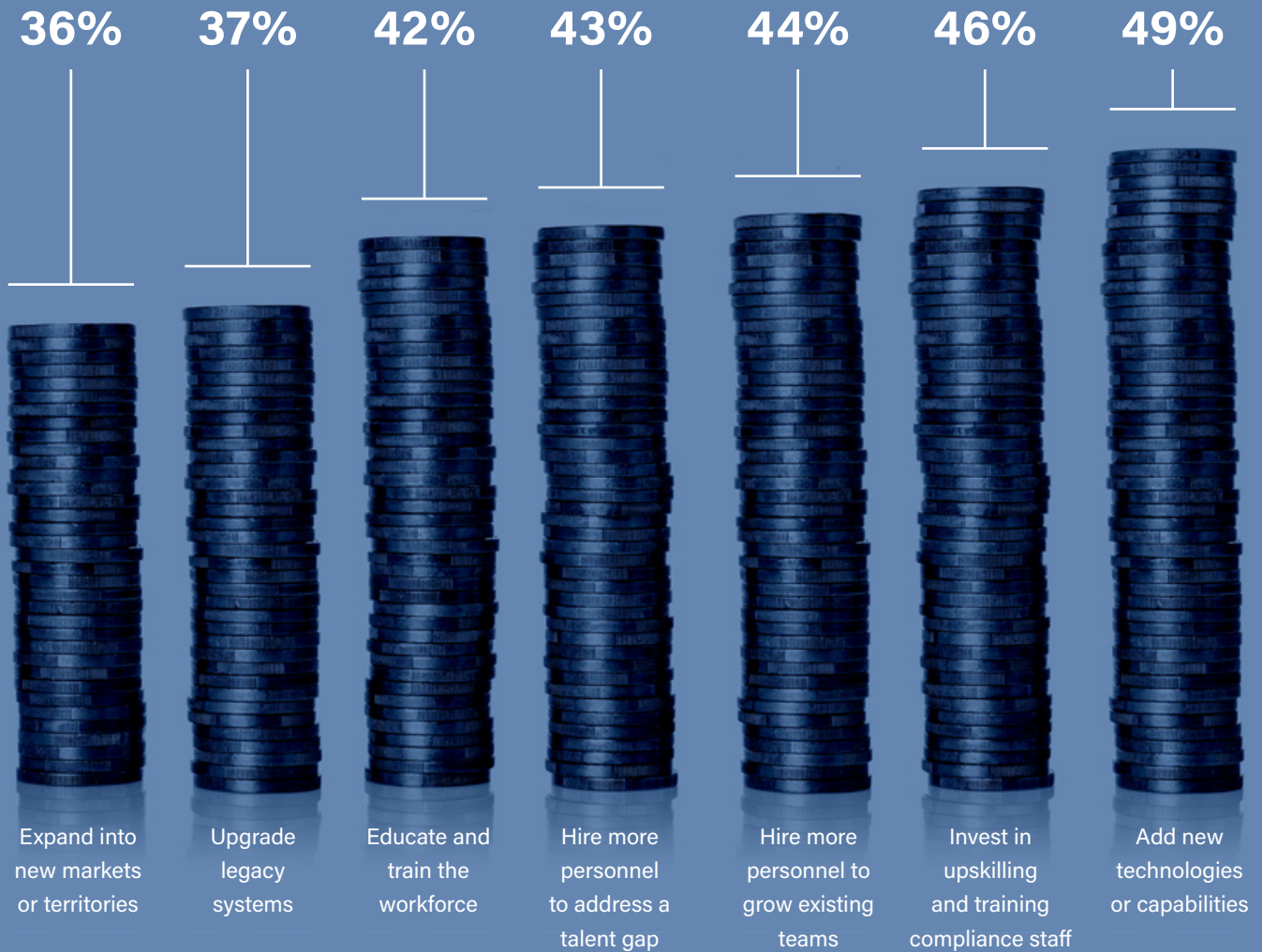
The rising cost of compliance and the need for highly skilled teams

As the world continues to experience some of the most complex geopolitical and economic shocks in recent history, financial crime teams must become increasingly alert, responsive, and agile to counter emerging threats and navigate unforeseen disturbances. While the global economic downturn is squeezing budgets, a swathe of new and more complex regulations are being introduced. At the same time, governments continue to rely on financial institutions to implement sanctions and fight financial crime in support of foreign policy objectives and law enforcement action

Meanwhile, the payments landscape continues to evolve, becoming more complex and digitized, with a greater variety of payment rails and different ways of making payments emerging to address consumer demand. We are also seeing a convergence between money laundering and cybercrime as criminals seek to launder their ill-gotten gains, while artificial intelligence (AI) has emerged as both friend and foe in the fight against financial crime. There is also an increasing convergence between cybercrime and money laundering. Nevertheless, firms can't take their eyes off traditional crime types that generate illicit finance, such as drug, arms, human and illegal wildlife trafficking, environmental crimes, and bribery and corruption, with different crime types more prevalent in different regions worldwide. All of this is creating different ways for criminals to target new victims, new pathways into organizations, and strategies to exploit the formal financial system that compliance teams in regulated firms must address.

Firms must invest in technology and highly skilled teams with individuals who can navigate hostile threats alongside regulatory changes and technological innovations. In our 2024 State of Compliance survey, almost all respondents

indicated that they would be increasing compliance budgets, with a clear focus on investing in personnel, technology, training, and enhancing capabilities. Respondents indicated that they would use their budgets as follows:



Source: ComplyAdvantage, The State of Financial Crime 2024

What does this mean for my firm?

Financial crime prevention teams must continue innovating and employing multi-layered approaches to fighting financial crime. This involves using more data, technology, and financial intelligence sharing to prevent, detect, and report illicit financial flows. Financial crime prevention teams must also continue to learn about emerging technologies, including threats and opportunities, and be able to support a workforce that should be trained continuously to remain able to detect financial

crime and potential sanctions breaches. Demand for skilled labor and technology solutions remains high, as do governments' expectations for their regulated firms. All of these factors combined will continue to drive up the cost of financial crime compliance in the near future.



Andrew Davies

Global Head of Regulatory Affairs,
ComplyAdvantage

Innovations in the payments landscape

The drive for innovation in the payments landscape continues in a post-COVID world driven by digitization combined with consumer demand for faster, more convenient payments and near-instant access to goods and services. Open banking, contactless payments, digital wallets, buy-now, pay later (BNPL) schemes, and digital currencies are all improving the customer experience but creating significant challenges for financial crime compliance. Open banking continues to take the world by storm through application programming interfaces (APIs) to share data between financial institutions and third-party service providers to make instant (real-time) payments. Over 60 countries have introduced an instant payment system based on different models, such as centralized or decentralized APIs, with varying degrees of regulatory involvement.

In our global survey,

46%

of organizations shared that they were already part of a real-time payments program,

44%

indicating that they have plans to join a real-time payments program.



By 2030, the open banking market is expected to hit [\\$135 billion](#), with the UK and the EU front and center. [Over 60 percent of the population is expected to use open banking in the UK by the end of 2023](#), and by 2024, it is estimated that there will be [63.8 million](#) open banking users in Europe. India's Unified Payment Network processes nearly [10 billion](#) monthly payments and will account for 90 percent of retail digital payments by 2027. The United States Federal Reserve launched its [FedNow](#) real-time payment rails, with real-time transactions expected to hit [\\$8.9 billion](#) by 2026. In Asia, Singapore has led the way in open banking with the Monetary Authority of Singapore issuing guidance, launching initiatives such as the [API Exchange \(APIX\)](#), and publishing a [register](#) containing 1702 APIs. [Nexus](#) has been created to connect the instant payment systems of the Eurozone, Malaysia, and Singapore, which could allow cross-border instant payments.

By 2027, the number of instant payment transactions globally is estimated to surpass [235 billion](#) from an estimated [74 billion](#) in 2023.

There has also been a consistent move towards contactless payments, mobile banking, and new payment schemes. This includes making payments by tapping cards, smartphones, and digital wallets offered by providers such as GooglePay, ApplePay, and wearable devices. This, combined with the proliferation of devices with near-field communications (NFC) technology, is leading to the continued growth in the use of mobile phones to accept payments. It is anticipated that by 2027, transactions associated with contactless payments will amount to [\\$10 trillion](#), with the global [market size](#) set to be valued at around \$165.15 billion by 2030. In the [UK](#), contactless fraud rose by 82 percent, card ID theft increased by 97 percent, and lost and stolen cards generated £100.2 million in losses, likely due to people being more in contact post-pandemic. The use of mobile banking and digital wallets will continue to grow. The Central Bank of Nigeria has recently announced a drive for a "cashless economy," and in other [African](#) countries such as Kenya, Ghana, and Tanzania, mobile wallets and mobile payments infrastructure are interoperable and seemingly everywhere. Services such as "buy now, pay later" (BNPL) are also becoming mainstream, making it easier for consumers to spread the cost of low-value goods over several months with no credit checks carried out. By 2027, [900 million](#) people will sign up for BNPL payments. There has been an increase in the use of BNPL for [theft](#) as criminals use legitimate user accounts to order goods on credit.

In the digital assets space, as countries regulate crypto assets, it is anticipated that more traditional financial institutions will move into this space. Companies like [Mastercard](#) already have a crypto card program and partnerships with exchanges like Tap, Nexo, and Gemini. Banks like Standard Chartered Bank, BNY Mellon, and Societe General already offer crypto custody services. [Deutsche Bank](#) recently announced it would provide crypto custody services for its institutional clients and tokenized assets. More countries are exploring [Central Bank Digital Currencies \(CBDCs\)](#), with over 130 countries currently comprising 98 percent of global GDP now in this space. [China's](#) CBDC has 260 million users. India is set to use its CBDC for call money settlement and, by the end of 2023, will look to process 1 million transactions per day.

In the non-traditional finance space, it is anticipated that more companies like [X \(formerly known as Twitter\)](#) will follow the footsteps of companies like [Uber](#), [Facebook/Meta](#), etc., and look to develop payment platforms facilitating in-app purchases or purchases via social media platforms, looking to enter the financial services space. This will require firms to transform how they accept users onto their platforms and may trigger AML/CFT compliance requirements. Telecommunications firms, car dealerships, and others

are also expanding the scope of their work and, therefore, increasingly need to manage their money laundering and sanctions risks.

While these innovations are welcome, firms must re-think how they fight financial crime. Not only is the volume of payments and transactions that must be monitored across different payment systems increasing, but so is access to the traditional financial system via different avenues. There is also a lack of data standardization and regulatory divergence on how customer due diligence checks and monitoring should be carried out for real-time payments, mobile payments, and payments and services offered in apps. Information previously seen by banks may also be reduced as transactions are processed via third parties using an API structure. The ability to stop fraud and money laundering in real-time or via mobile apps remains challenging. In the UK, the payments services regulator has introduced confirmation of Payee (CoP) on instant payments to check that account name and details match to address advanced push payment fraud and prevent accidental payment errors. Also, Mule Insights Tactical Solutions was rolled out by Pay.UK to detect real-time fraud and mule accounts. Firms looking to enter the payments space must consider applying European requirements around strong customer authentication (SCA). SCA was introduced by the Payment Services Directive 2, requiring payment firms to obtain a [combination](#) of the following from their users when making payments: something they know (password, pin, passphrase, or secret fact), something they own (such as mobile, smart card, wearable device, token) and something they are (verified using biometrics such as fingerprints, face, voice patterns, iris, phone holding patterns).

What does this mean for my firm?

Firms need to rethink how they fight financial crime. They will need to re-assess how to monitor an increasingly challenging payments landscape with multiple payment rails worldwide. They will need to ensure that they can stay on top of emerging payments legislation, best practices, and guidance issued around emerging payment models.



Alia Mahmud

Global Regulatory Affairs Practice
Lead, ComplyAdvantage

The rise of AI and the convergence of cybercrime & money laundering

AI continues to emerge as both a friend and foe in the fight against financial crime.

On the one hand, AI is being deployed by criminals to perpetrate fraud, launch attacks against individuals and corporations, and gain access to the international financial system. AI has been linked to inciting [terror attacks](#), generating deepfakes for ransom, extortion, and fraud, carrying out corporate espionage, the dissemination of child sexual abuse materials (CSAM), and carrying out online account takeover fraud for profit. Criminals have the ability to perpetrate further crimes using AI-enabled

[data poisoning](#), [snake oil](#), [burglar bots](#), [online eviction](#), [market bombing](#), [tricking fake recognition](#), and forgery. Once criminals have found an application for AI, it can be easily shared, repeated, and sold, creating a new model for "[Crime as a Service](#)." Alarm bells have also been rung around the existential threat posed by "societal-scale disruptions" caused by AI in the future or "[artificial general intelligence](#)" (AGI), which is effectively AI that matches human-level performance. The UK recently hosted an international AI Safety Summit, bringing together government and business leaders, including the US and China. This led to a [commitment](#) to test large language models with the government to guard against national security and societal harm and promote safety.

At the same time, AI is increasingly being deployed in solutions such as customer onboarding, adverse media and sanctions screening, transaction monitoring, and automated reporting to regulators. AI-based solutions can offer massive efficiencies and make the fight against financial crime more effective by reducing false positives, enriching customer data, and identifying new risks. On a global basis, the AI market was anticipated to reach [US\\$241.8 billion](#) by the end of 2023. A growing area of major concern and focus is the concept of [explainability](#), or the ability to explain how AI works or how and why an AI model generates decisions or outcomes. [Regulators](#) are increasingly looking to those using or providing AI models to have clear and understandable information on the AI model's capabilities and limitations and transparent and traceable decision-making processes.

Our State of Financial Crime 2024 survey reveals how firms are thinking about AI. At times, it often appears contradictory. Many firms are comfortable trading off explainability to improve efficiency, while at the same time believing they're on track to meet regulators' expectations:

89%

are somewhat comfortable compromising explainability in exchange for greater automation and efficiency.

68%

say they have a good understanding of how legislators and regulators plan to regulate AI technologies.

66%

of firms agree that the development of AI poses a growing cybersecurity threat.

59%

say they are well prepared to meet proposed AI legislation, with 39 percent somewhat prepared.

Over
50%

of firms are concerned about being able to explain decisions and/or outcomes of AI-based financial crime solutions to a multitude of stakeholders, including customers, internal stakeholders, investors, and regulators.

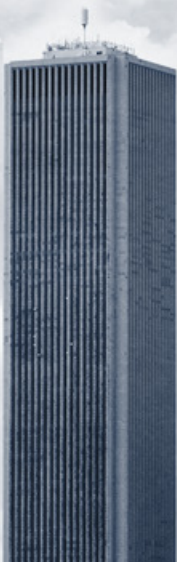
Privacy-enhancing technologies (encrypted messaging apps, dark web marketplaces, and digital assets) will continue to protect the identity of criminals and allow for increased collaboration. Data volumes continue to increase, with [100 zettabytes](#) of data stored in the cloud worldwide by 2025. By 2027, the number of connection points across the [Internet of Things](#) will almost double to 29 billion, generating “almost unlimited” digital attack surfaces that criminals can use to launch ransomware, identity, or data theft strikes. By 2031, [ransomware victims will lose \\$265 billion](#), with attacks expected every two seconds. Cybercrime is anticipated to cost [\\$9.5 trillion](#) in 2024. Additionally, criminals will continue to exploit weak IT protocols, set up fake investment websites, target e-commerce businesses, and carry out social engineering scams, including phishing, smishing, and vishing. Synthetic identity fraud, including that created from stolen data, will remain the largest form of identity theft, which is harder to detect when used online. Losses related to online fraud, including authorized push payment fraud and unauthorized transactions, remain high, with consumers losing [£1.2 billion](#) in the UK in 2022. It is

interesting to note that our survey suggested 60 percent of firms surveyed indicated that instances of payment fraud stayed the same or decreased over the last 12 months. However, although, this reflects fraud rates that which remain at historically high levels.

The rise of digital banks offering online services and the deployment of new products, such as the use of virtual IBANs, also hide key information, making them targets for criminals. Cryptocurrencies, particularly those with privacy-enhancing layers, will continue to remain susceptible to misuse by criminals as the technological adoption grows until there is concrete regulation in place. The [metaverse](#) is another frontier that could be exploited by criminals with concerns around privacy and security being compromised, such as biometric data, manipulation through avatars, the theft of virtual property, and human-like interaction that could lead to fraud, scams, and radicalization. Law enforcement has already [identified](#) significant increases in criminal activity in immersive environments. These developments accelerate the need for firms to step up their cybersecurity strategies.

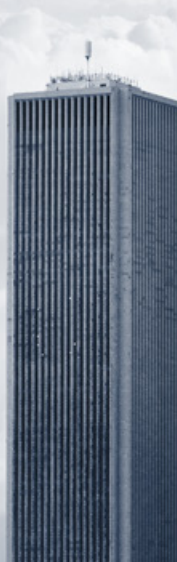
87%

of firms are hiring new staff to handle the increasing number of cybersecurity threats.



86%

are investing in new technology to combat rising cybersecurity threat instances.



88%

of firms are investing more in response to rising cyber threats.



87%

of organizations are reallocating resources to focus on cybersecurity.



What does this mean for my firm?

Firms should ensure that they remain abreast of guidance and international agreements around AI. Compliance leaders exploring AI solutions should ensure they understand and document the rationale behind exploring a solution and have the right clean data to train AI models. Documentation proving that they understand how the AI models work is also essential. Finally, firms should break down the silos between their financial crime compliance teams and cybersecurity teams to identify risks across the organization.



Iain Armstrong

Regulatory Affairs Practice Lead,
ComplyAdvantage

Bribery, corruption, and PEPs

In 2024, the geopolitical and economic landscape is set to become more unpredictable, with over 40 countries holding elections. This will make the PEP environment even more complex, as allegations of corruption, money laundering, and judiciary intervention could emerge as part of political posturing. The electoral results could have implications for sanctions and, in some cases, either strengthen or weaken the resolve of countries to tackle illicit financial flows.

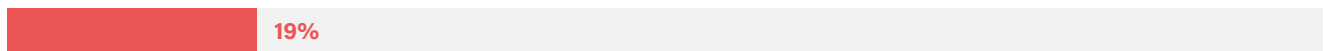
Firms are clearly braced for a year of uncertainty. 61 percent of compliance leaders told us they plan to become more risk-averse when managing PEPs over the next 12 months. 73 percent also said they would need to reduce their reliance on manual screening processes, indicating potential technological hurdles firms need to overcome before the 2024 election season ramps up.

How do you expect your organization's risk appetite related to politically exposed persons (PEPs) to change in the next 12 months?

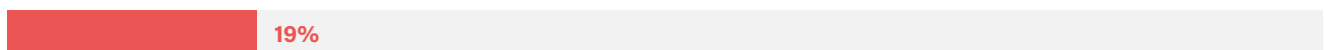
More risk-averse (e.g. greater due diligence at onboarding and ongoing monitoring)



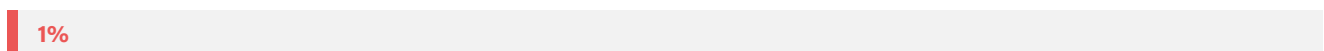
No Change



Less risk-averse (e.g. reduced due diligence requirements)



We are not accepting PEP clients

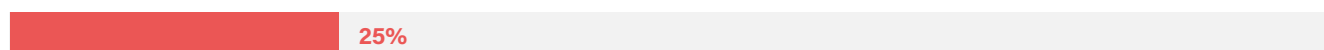


Do you expect national elections planned for 2024 (e.g., US, UK, India) to impact the way your organization manages PEPs?

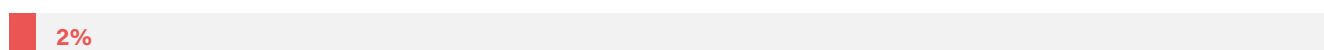
Yes - we'll need to reduce our reliance on manual processes to reassess this volume of PEPs



No - our existing technology can handle expected changes in a reasonable timeframe



Not sure - we haven't evaluated the impact



At the same time, global levels of alleged bribery and corruption continue to grow.

98%

of firms in our survey indicated that detecting and preventing corruption is a strategic priority for their organization's financial crime compliance function.



It should remain so given the many corruption cases emerging worldwide, associated illicit financial flows, and signaling by many countries to clamp down on corruption.

All eyes are on US elections in November, which could have significant implications for global peace and stability. Whether Donald Trump can take on President Joe Biden in what is expected to be a very tight race remains to be seen. Former President Trump, whose popularity has risen following charges issued against him, [faces over 90 criminal charges](#), including racketeering and fraud, allegations of mishandling [classified documents](#), trying to overturn the 2020 election, and falsifying records. President Biden's son, Hunter Biden, has also been investigated for using his father's name to advance his [business interests](#) in Ukraine and China while his father was Vice President. New Jersey Senator Robert Menendez, who chaired the Senate Foreign Relations Committee, his wife, and three businessmen were [charged with corruption](#)

In 2024, we will see a great deal of political activity. Many countries are due democratic elections, and many ruling parties are expected to change. That means that many politically exposed persons will find themselves out of office, while many, many people will find themselves newly classified as PEPs, along with their close family and associates

With this level of change going on, banks and other firms who have obligations to monitor the financial dealings of PEPs closely will find a large uptick in the work they have to do on a day-to-day basis for these accounts. And the account holders might find their transactions unduly delayed or hampered if firms aren't knowledgeable enough about their customers' dealings and must keep making inquiries and investigating in real time. So, dealing with a large volume of incoming and outgoing PEP designations will be a challenge in the coming year that firms should be preparing for now.



Graham Barrow

Director, The Dark Money Files Ltd



Ray Blake

Director, The Dark Money Files Ltd

linked to bribes received to benefit the Egyptian government. Across the Atlantic, the UK must hold elections by January 2025, with opposition party leaders vowing to track down billions lost to COVID-19 fraud. The UK, which has had three prime ministers since the last election, has been afflicted by a series of corruption scandals, including 'Partygate,' which forced Boris Johnson to resign over parties held by his staffers during lockdowns, the allocation of contracts to persons connected to the ruling party and the awarding of roles in the public sector to persons connected to politicians. The UK also recently commenced a review of the treatment of domestic PEPs by banks following the de-banking of politician Nigel Farage and allegations of improper conduct that led to the resignation of the CEO of Natwest. The FCA will issue its report by the end of June 2024.

The European Parliament, still reeling from 'Qatargate,' is set to hold elections in June. The scandal, which revolves around a cash-for-influence scheme with MEPs allegedly receiving bribes from Qatar, Morocco, and Mauritania, has led to the arrests of several high-profile EU parliamentarians, including former Vice President and Greek MEP Eva Kaili. Other countries holding leadership races on the European continent include Austria, Belgium, Croatia, Finland, Georgia, Iceland, Lithuania, Moldova, Romania, and Slovakia. In Austria, former Chancellor Sebastian Kurz, who was surrounded by allegations that he used public funds to bribe pollsters and journalists to support his political agenda, was indicted for making false and misleading statements linked to the 2019 Ibiza scandal. There are also concerns related to more far-right parties taking control, Russian meddling in elections, and a rise in populism. Ukrainian President Zelensky is also weighing up the pros and cons of holding elections in 2024, although martial law currently forbids this. Several countries are considering tying development assistance to anti-corruption and good governance measures. Zelensky has dismissed officials surrounded by allegations of corruption and cronyism, including his minister of defense. Russia is due to hold a presidential election in May, although it is unlikely to result in a change in leadership. France has submitted a proposal to create an EU anti-corruption body that would identify conflicts of interest and check the income of public officials.

Taiwan is set to launch the 2024 elections calendar, holding presidential elections in January. Taiwan is a major geopolitical flashpoint due to an increased Chinese military presence in the South China Sea and the potential for this to lead to conflict between the US and China. It has also triggered sanctions. Legislation has been put forward in the US, requiring sanctions to be applied if China were to

invade Taiwan. Taiwanese elections, however, could offer the opportunity for renewed dialogue between Taiwan and China. Taiwan is still reconciling its corrupt past, with the former President's son, Chen Chih-Chun, imprisoned for one year for hiding illicit funds overseas linked to corruption cases involving members of the former first family, embezzlement, and abuse of authority. China has ramped up anti-corruption efforts, with 36,000 recorded cases in the first half of 2023, and launched a year-long, "unprecedented" multi-agency crackdown on corruption in health care.

Other scheduled elections include Indonesia in February, India in April, South Africa in May, and Mexico in June. In Indonesia, there is a possibility of a return to authoritarianism as President Joko Widodo was barred from running for a third term. In India, Prime Minister Narendra Modi has launched his campaign pledging to fight "corruption, dynasty and appeasement." This is against a backdrop of the ongoing investigation of the multimillion-dollar collapse of Jet Airways and billions of losses triggered by fraud allegations against the Adani Group that triggered a banking crisis and fears of contagion in India. In South Africa, President Cyril Ramaphosa was cleared of 'Farmgate,' a scandal that involved allegations of wrongdoing for failing to report the theft of up to \$4 million in cash from a couch on his farm. He indicated that the funds came from the sale of cattle to a Sudanese businessman, although the police continue to investigate. Mexico's current President, Andrés Manuel López Obrador, plans to slash the budget of the electoral watchdog, which could lead to a loss of 85 percent of its staff ahead of the elections. He has also accused protesters of being linked to drug traffickers. President Obrador's son has been surrounded by allegations of corruption involving allocating public contracts to friends and families, including building on protected land.

Politically unstable countries such as Venezuela, Pakistan, and South Sudan are also due to hold elections. In Venezuela, the attorney general launched an investigation into alleged financial crime and conspiracy to suspend the results of the primaries where María Corina Machado was elected to run as the opposition candidate against President Maduro. Although the US lifted some sanctions following a deal to hold elections in Venezuela, authorities have indicated that transnational criminal organizations, terrorist organizations, and illicit finance have continued to thrive due to the corruption, economic turmoil, and political instability that have characterized President Maduro's tenure. Pakistan, a nuclear power, is set to hold elections early next year under the auspices of a caretaker government led by Prime Minister Anwaar-ul-Haq Kakar that was set up following a

no-confidence vote in April 2022 against former Prime Minister Imran Khan. This was followed by the arrest of thousands of members of Khan's party after he allegedly fell out with the military and was convicted of corruption and charged with sedition. Khan is banned from running for office for five years. South Sudan is set to hold its first-ever election, with President Salva Kiir set to run against long-term rival Riak Machar. The country is plagued by systemic corruption, with numerous allegations of misappropriation of state funds and political capture of the banking system, and the previous conflict between Kiir and Machar led to the death of over 400,000 people.

What does this mean for my firm?

Firms should have a list of PEPs whose accounts should be monitored, particularly if they are up for election. They should identify markets in which they operate that may be affected by elections and monitor for regime change and capital flight. Financial crime compliance teams should also liaise more closely with anti-bribery teams to identify any potential conflicts of interests and key anti-bribery controls that should be in place to limit the chances of their firms being used to launder proceeds of corruption. Finally, firms should continue to carry out enhanced due diligence on PEPs and remain vigilant of the misuse of corruption for political interference.



Alia Mahmud

Global Regulatory Affairs Practice
Lead, ComplyAdvantage



Regional Trends

The Americas

The US will continue to face threats from abroad and at home.

Crypto became a major focus with the trial of former FTX CEO Sam Bankman-Fried (SBF). SBF was found [guilty of fraud](#), money laundering, and conspiracy, with the fall of FTX leading to the loss of billions of dollars. The identification of the use of crypto to finance terrorism by Hamas following the Israeli terrorist attacks added further scrutiny. A Gaza-based [crypto exchange](#) found to have transferred funds to Hamas has been subject to sanctions in the US, with legislators taking increasing action against crypto, including recent indications that FinCEN may designate all [crypto mixers](#) as being of “primary money laundering concern.”

The Biden administration also released the world’s first [DeFi Illicit Finance Risk Assessment](#). As of December 2022, DeFi’s [total value locked](#) was estimated at \$39.77 billion. The report cited the limited application of AML/CFT obligations to DeFi, lack of global harmonization, the disintermediation of DeFi services, limited regulation of DeFi, and poor cybersecurity practices as key vulnerabilities. DeFi has also been used to launder money by nefarious actors, including those based in North Korea, generating exposure to proliferation finance. Law enforcement has also identified the use of DEXs and cross-chain bridges, mixers, and liquidity pools to launder funds. DeFi has been linked to ransomware attacks, theft of virtual assets, fraud and scams such as rug pulls and pig butchering scams, and drug trafficking.





Additional threats facing the US include drug trafficking, human smuggling, and terrorism linked to Mexican drug cartels that are increasingly posing a hybrid threat with links to overseas associates. Following the Matamoros murders of US citizens by the Gulf Cartel in Mexico, US senators introduced legislation, the Ending the Notorious, Aggressive, and Remorseless Criminal Organizations and Syndicates ([NARCOS](#)) Act, to designate nine Mexican cartels as Foreign Terrorist Organizations (FTOs). This would allow the use of greater [powers](#) to freeze assets, target individuals providing material support, and ban entry into the US. However, there are concerns of rising rhetoric on the use of US [military action](#) in Mexico against cartels. The Sinaloa Cartel and the Jalisco Cartel are the primary distributors of fentanyl in Mexico and have control over smuggling corridors. A recent US [indictment](#) highlighted that Mexican Cartels were using Chinese chemical companies that supply fentanyl precursors, fentanyl analogues, xylazine and nitazenes, amongst others. These Chinese companies used US-based re-shippers, false return labels, fraudulent portaging, and false invoices to conceal what was being shipped. Fentanyl has been identified as being 50 times stronger than heroin and 100 times stronger than morphine and, since February 2022, has been linked to the [deaths](#) of over 100,000 people. Twelve individuals were indicted in April 2023 for laundering funds for the Sinaloa Cartel and a national of Belize who used a network of [cash couriers](#) to move funds throughout Latin America and the US.

In August, the US and Mexico held a Strategic Dialogue on Illicit Finance ([SDIF](#)) to discuss how to counter drug, arms, and human trafficking. The US also recently released a [2023 Trafficking in Persons Report](#), taking stock of human trafficking around the world, with the top three [countries of origin](#) identified as the US, Mexico, and Honduras. The report also included a list of countries involved in the state-sponsored trafficking of persons. The main terrorist threats come from foreign terrorist organizations such as ISIS, Al-Qaida, and Hizbollah, including the radicalization of individuals in-country, as well as the threat of domestic violent extremism. Given the [2024 elections](#), there are concerns that online calls for violence or violent extremist messaging could heighten the threat of terrorist acts in-country. Domestic terrorism-related investigations have increased by [357 percent](#) over the last 10 years.

Canada published an updated [national risk assessment](#) on money laundering and terrorist financing, citing threats that firms should be aware of. The following crimes were rated as posing a very high threat of money laundering:

- Capital markets fraud
- Fraud
- Illicit drug trafficking
- Commercial (trade) fraud
- Mass marketing fraud
- Corruption and bribery
- Mortgage fraud
- Illegal gambling
- Third-party money laundering

Crimes representing a high threat include:

- Currency counterfeiting
- Payment card fraud
- Counterfeiting and piracy
- Pollution crime
- Human smuggling
- Robbery and theft
- Human trafficking
- Tax evasion/tax fraud
- Identity fraud
- Tobacco smuggling and trafficking

Canada will also continue to struggle with ideologically motivated violent extremists (IMVE), with around 50 percent of Canadian Security Intelligence Services allocated to investigate cases of IMVE. Canada will continue to address [“snow washing,”](#) or illicit finance into Canada to evade taxes or fund terrorism, as well as the misuse of real estate to launder money.

Latin American countries will continue to face challenges with drug trafficking, migrant smuggling, and terrorist financing. Structural [weaknesses](#) have been identified as poor governance, major inequalities, and informal economic systems that allow illicit finance to flourish. The IMF flagged that the presence of [transnational criminal gangs](#), which are connected to organized crime groups in Europe, the US, and Africa, are harming economic growth and investment. These groups have also grown trading routes to smuggle drugs and humans to countries such as Ecuador, Chile, Paraguay, and Uruguay. In Columbia, [illegal gold mining](#)





has been linked to organized crime groups and identified as an emerging threat. 85 percent of gold production out of Columbia comes from illegal mining, with 66 percent taking place in natural parks and country reserves, contributing to environmental crimes. Columbia is also facing a major scandal following the arrest of President Gustavo Petro's son and charges of [money laundering](#) and illicit enrichment from individuals linked to drug trafficking.

[UNCTAD](#) issued the first official estimate of illicit finance flows with the following data available for Latin American countries:

Mexico – Drug trafficking (such as heroin, cocaine, and methamphetamine) generated an estimated \$12 billion of illicit financial flows into Mexico annually between 2015 and 2018, with migrant smuggling generating \$1.1 billion into Mexico and \$13.8 million out of Mexico annually between 2016 and 2018.

Colombia – Cocaine trafficking poured between \$1.1-8.6 billion into Columbia each year between 2015 and 2019 and between an estimated \$197 million and \$267 million each year between 2015 and 2019 out of Columbia.

Ecuador – The smuggling of migrants generated approximately \$13.6 million annually out of Ecuador between 2016 and 2018.

Peru – Illicit finance linked to cocaine trafficking into Peru generated approximately \$1482 million each year between 2015 and 2017.

Haiti was identified as the country most at risk of money laundering and terrorist financing in the world by the [Basel AML Index](#). Haiti acts as a transshipment route, which is overrun by [armed criminal gangs](#) often supported by the political elite and business leaders. The US recently [sanctioned](#) companies and financial facilitators based in several Latin American countries, including El Salvador, Venezuela, and Colombia, used to launder proceeds of drug trafficking and other money laundering activities for Hezbollah.

Europe

Europol published its [first threat assessment](#) of financial and economic crimes in Europe. It identified three key drivers of financial and economic crime, including serious and organized crime, digital acceleration, and geopolitical development, focusing on the links between sanctions evasion and organized crime. It highlighted that around

70% of criminal networks employed basic money laundering techniques,

with 80% of crime involving the misuse of legal business structures (shell companies, complex structures, cash-intensive businesses)

and 60% including some form of corruption.

Areas of concern cited include the growth of cybercrime, migrant smuggling, fraud, and diversion of goods. The report also highlighted the convergence between organized crime and sanctions evasion, with concerns about a rise in the use of money mules to raise funds. Sanctions evasion methods shared include disguising beneficial ownership, using intermediaries and fraudulent documents, and relocating and undervaluing assets.

The EU also identified the [use of third countries to conceal the involvement of Russia-origin transactions](#), the rise of money laundering-as-a-service to assist sanctioned persons, and a rising trend in cash smuggling in and out of Europe into Russia. The EU estimates that 30 percent of criminal networks operate with the underground banking system





which, alongside professional money laundering networks, fuel the rise of money laundering-as-a-service. This includes the provision of cross-border funds transfer services, sometimes via informal value transfer systems, and insurance to guarantee the delivery of funds. Trade-based money laundering, the potential for digital assets to be misused given the growth of online and offline activity, the rise of criminal finances, and the investment of criminal assets into the economy were also raised as areas of concern. Fraud remains a major issue. Different types of fraud referenced include online fraud, business email compromise fraud, e-commerce fraud, tech support fraud, investment fraud, (particularly in the cryptoasset space), romance fraud, recovery of refund scams, mass mailing, and food fraud perpetrated against individuals. Types of fraud against the EU and member states include subsidy, excise, customs import, VAT, and fraud linked to sporting events. Intellectual property crime has been seen infiltrating every step of the legal supply chain, with counterfeit goods coming from abroad and a rise in currency counterfeiting.

The European Banking Authority (EBA) recently published its [Opinion](#) on the risks of money laundering and terrorist financing affecting the EU's financial sector. Particular emphasis is placed on the changed risk landscape due to Russia's invasion of Ukraine and technological innovation. Key risks include the laundering of the proceeds of corruption, environmental crime, human trafficking, and cybercrime. Risks that remain relevant include those associated with crypto assets, innovative financial services, a lack of beneficial ownership transparency, and terrorist financing. Europe has also been identified by [Interpol](#) as one of the "main transit and destination markets" for illegal drugs, with a rise in "violent crime, corruption and money laundering of unprecedented scale" around European borders and ports. Online child sexual exploitation and abuse are expected to increase in Europe in the next three to five years.

Due to the Cyprus Confidential leaks, significant attention will remain on the country. Recent reports have exposed the use of Cypriot enablers, including bankers, accountants, auditors, and lawyers, to hide and launder billions of assets for Russian oligarchs. Reporting has revealed that following the invasion of Ukraine, Cypriot firms and lawyers were used to restructure the assets of Russians to limit the effect of Western sanctions, with more than 650 registered trusts and companies owned or controlled by sanctioned Russians. The Western Balkans have also been identified as an illicit finance hotspot, with illicit financial flows in the Balkans estimated at equaling [6 percent](#) of Europe's GDP. This has been attributed to state capture and institutional weaknesses.

Asia

In Asia, one of Singapore's largest money laundering cases will continue to dominate headlines in 2024. Authorities will make further arrests, seize more assets, and more banks are likely to be implicated in the scandal worldwide.

In August 2023, law enforcement authorities began seizing assets, including luxury real estate, jewelry, gold, vehicles, and designer bags, valued at more than \$2.8 billion.

The case has been linked to a Chinese [online gambling racket](#), which had previously operated in the Philippines and Cambodia, and the criminal syndicate [Heng Bo Bao Wang](#). Major [banks](#) in Singapore, Europe, and China have been identified as having exposure to the case, and an inter-ministerial panel will review Singapore's anti-money laundering regime with authorities indicating that they would be conducting on-site supervisory visits of banks.

Chinese operators will continue to feature in [money laundering](#) operations with recent arrests of Chinese money launderers in cases in Australia, India, Italy, and Spain linked to local organized crime groups. China has been cracking down on illegal online gambling, which has resulted in live streaming and chat apps being suspended "for [business adjustment](#)." In 2020, Chinese authorities cited the cross-border transfers associated with gambling as a [national security risk](#), and the Ministry of Public Security recently indicated that authorities solved 6,800 online gambling [cases](#). China issued a warning to Chinese chemical companies that make [fentanyl precursors](#), indicating that they could face criminal charges. Australian police arrested members of Chinese money laundering syndicate Long River, which used money services remittance businesses to launder over [\\$140 million](#) generated from cyber scams, violent crimes, and trafficking in illegal goods. It is alleged





that they used counterfeit invoices and created fake bank statements alongside other business documents. China has also recently taken action against a multi-billion dollar [telecoms fraud](#) industry run by armed groups in Myanmar and staffed by workers often held against their will. There are an estimated 120,000 people working in scam rooms and living in deplorable conditions in Myanmar.

North Korea will remain a challenge, with state-sponsored groups continuing to pose a major cybersecurity threat. North Korean [actors](#), described as “sophisticated and agile,” have engaged in ransomware attacks, espionage, cryptocurrency heists, and used mixers to launder funds to finance its [nuclear arms](#) and ballistic missiles program. Over [\\$2 billion](#) is estimated to have been stolen from crypto exchanges and banks over the past five years, with nearly \$150 million stolen in 2023, including the Atomic Wallet attack in June 2023 and the September breach of decentralized project [Mixin](#). US authorities have also warned of attacks on healthcare and other critical infrastructure. North Korea has been identified as [smuggling arms](#) to Russia and other countries, including Iran and Syria, with China acting as a transshipment center to third countries. In September 2023, South Korea imposed [sanctions](#) on individuals and entities involved in illegal financial transactions associated with North Korea's nuclear program and arms trade.

Firms should remain aware of the sanctions circumvention risk of Central Asian countries due to a high dependence on China and close economic ties with Russia. Countries such as Kyrgyzstan, Kazakhstan, Georgia, and Armenia have acted as [re-exporters](#) through the EU, which are likely to have been used to evade sanctions by Russia. Reporting indicates that drug trafficking through Central Asia “is significant,” with evidence that the [political elite](#) is “involved in, and controlling, drug trafficking routes.” The UK and Europe are key destination countries for drugs from Central Asia. In India, the [Adani Group scandal](#) erupted, wiping out billions of dollars of value in the stock market and raising fears of banking contagion following allegations of stock manipulation. The Adani Group is a massive conglomerate that has received many government tenders and is seen as being central to Prime Minister Modi's plans for redevelopment.

A recent [Interpol](#) study found that across Asia, there will likely be an increase in the trafficking of synthetic drugs alongside cybersecurity attacks, including ransomware, phishing attacks, business email compromise, identity theft, and online extortion. Environmental crimes will also generate profits for Asia's criminals, with Vietnam, Laos, Myanmar, and Cambodia identified as key trafficking hubs for [endangered species](#), including tigers and pangolins. China will remain a major consumer market for illegally trafficked protected species as well as illegally traded timber.

Middle East & Africa

Certain countries in the Middle East and Africa are likely to remain hotspots for financial criminal activity, with regional instability increasing the threat of terrorism, human trafficking, and arms trafficking.

The UAE, Lebanon, Iran, and Iraq have been identified as having a high volume of financial criminal activity to such an extent that it is considered systemic.

The UAE is an international financial hub with a large trade in gold and diamonds, amongst other commodities, and has been used to circumvent sanctions. There are also [10,000 ISIS](#) detainees in Syria alongside tens of thousands of displaced children, which could lead to a future threat. Iran continues to pose a risk of nuclear proliferation and has been linked to financing terrorist attacks perpetrated by Hamas in Israel. In May 2023, G7 countries issued a statement warning of [illicit finance activities](#) posed by Iran.

Poor governance, regional instability, and vast inequalities will continue to expose Africa to a strong [criminal market](#) driven by human trafficking and arms trafficking. Africa is estimated to lose nearly [\\$60 billion](#) to illicit finance each year. Organizations such as the Wagner Group, which is fracturing into other private military groups following the death of its leader Prigozhin, set up [operations](#) in the Central African Republic, Mali, Sudan, Libya, Mozambique, and Madagascar. The group was designated as a terrorist organization by the UK government, and is said to be supplying Hezbollah with an [air defense system](#). The security situation in the Sahel and West Africa continues to deteriorate, with Africa identified as being "home to nearly half of global terrorism [deaths](#)."





Countries such as Eritrea and South Sudan have high levels of human trafficking, with conflict-riddled countries such as Sudan, Somalia, Ethiopia, and Djibouti identified as markets for [smuggling illegal weapons](#) alongside drugs and pirated goods. Wildlife trafficking and gold smuggling also remain major sources of illicit finance in the DRC. [Interpol](#) has also identified the use of explosive precursor chemicals and initiators to develop explosives in illegal mining and blast fishing in Central Africa and the trafficking of explosives into the DRC, CAR, Chad, and Cameroon by groups such as Boko Haram, the Islamic State and rebel groups for use in armed conflicts. Nigeria has seen an increase in mobile [fraud](#), computer and online fraud, and point-of-sale fraud. South Africa and the United States set up a [task force](#) to tackle wildlife trafficking in 2023, and South Africa is tackling a gold [smuggling](#) operation used by criminal gangs to launder billions of dollars and circumvent sanctions.

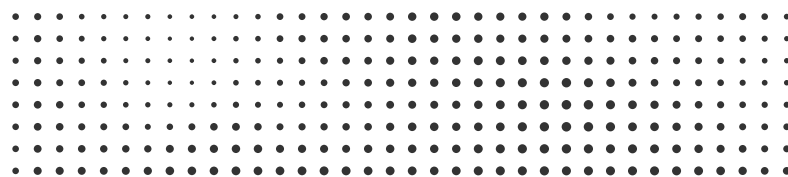
What does this mean for my firm?

Firms should ensure that they are carrying out horizon-planning activities to identify emerging regional trends. Compliance leaders should also engage in public-private partnerships to be able to share intelligence with law enforcement if and when they identify suspicious activity related to their clients. Firms should also update their business, customer, and product risk assessments to take into account money laundering and terrorist financing risks and develop the right controls to mitigate their risks.



Andrew Davies

Global Head of Regulatory Affairs,
ComplyAdvantage



- [↑](#) Back to beginning
- [←](#) Previous section
- [→](#) Next section

Geopolitics and Sanctions



In normal times, 2023 would have been seen as a busy year in geopolitics. But in the wake of the [Russian invasion of Ukraine](#) in February 2022 and the massive Western sanctions in response to it, 2023 has seemed relatively quiet by comparison. However, as the events in Gaza and Israel in the autumn of 2023 have demonstrated, new crises can emerge quickly.

At present, the prospects for 2024 are finely balanced. Some aspects of world politics suggest another year of relative stability. With the [US presidential election](#) taking up most of 2024 (election day being November 5), the US will likely be focused more on domestic than international issues. There is reason to believe that most major geopolitical hotspots will not worsen next year. After a mildly successful Ukrainian counter-offensive in the summer and autumn, the Ukraine conflict has hit a point of stalemate that points to eventual negotiations rather than further escalation. In the Middle East, too, Iran, Syria, and Hezbollah have so far largely held off from intervening in the war between [Israel and Hamas](#) in the Gaza Strip. North Korea is likely to continue to rattle its nuclear saber, but this is 'business as usual'. Most importantly, like the US, China remains preoccupied with domestic concerns such as [mixed economic news](#) and the rearrangement of President Xi's [senior team](#). While continuing with aggressive rhetoric against [Taiwan](#) and a friendly stance

toward [Russia](#), China appears to have taken few concrete actions that might stimulate an angry Western response. Circumspection seems to be the present mood in Beijing.

But these constraints should not lead us into a state of complacency. While the US might not want overseas trouble next year, events may follow a different course. A frontline collapse on either side of the Ukraine conflict, or a new coup in Moscow, might lead to escalation. In the Middle East, Hezbollah or Iraqi Shia militias might initiate military action that stimulates a wide-ranging Israeli response. Domestic unrest in Iran could lead to vicious repression. The outcome of the [Taiwanese presidential election](#) in January may stimulate an aggressive Chinese response, or China might be tempted to take action against Taiwan while the US is distracted by other issues. China might also feel obliged to provide material support to Russia if its defeat seems imminent. While these scenarios seem less likely on balance than 'more of the same,' we cannot rule them out. In any of these instances, Western countries will take a strong and coordinated response that will probably include new economic and financial sanctions. Indeed, it is important to register that – even though 2024 will probably not see a dramatic worsening of the world situation, it will also not see many improvements, except perhaps in isolated cases such as the [relaxation of US sanctions on Venezuela](#).



What are Sanctions?

Sanctions are restrictive measures international organizations and national governments apply to influence or punish other states and non-state actors, such as terrorists or organized criminals. They are typically applied to support international peace and stability and national security goals, but not exclusively, with their increasing use to target human rights abuses and corruption – commonly referred to as ‘Magnitsky’ sanctions after murdered Russian lawyer [Sergei Magnitsky](#). Nearly all countries follow the sanctions imposed by the [United Nations Security Council \(UNSC\)](#), but an increasing number also have autonomous regimes, of which the US is the most influential. Sanctions commonly target entities such as official institutions, businesses, groups, networks, and individuals. When imposing sanctions, sanctioning bodies commonly prohibit those under their authority from undertaking economic and financial interactions with the target or freeze its assets. Personal sanctions also now commonly involve travel bans to areas under the sanctioning body’s control or via carriers under its authority.



Major Hotspots: Russia

Our [State of Financial Crime Report 2023](#) suggested that the future of sanctions against Russia was “likely to hinge on developments on the battlefield in Ukraine itself.” This has largely been borne out by events where the Western sanctions regime has been largely stable and focused on filling gaps and removing loopholes. Nonetheless, this does not mean there has been no sanctions-related activity against Russia throughout 2023, with the year seeing an increasing focus on evasion via ‘neutral’ third-party countries. Although focusing on third parties has long been part of the US sanctions toolkit – so-called [‘secondary sanctions’](#) – their potential deployment by the European Union (EU) has been a marked departure from past practice.

The War in 2023

Despite Russia’s failure to defeat Ukraine in 2022, the Putin regime and the Russian military have remained doggedly determined to stay in the fight, with further major [troop call-ups](#) and extensive [drone strikes](#) against Ukrainian infrastructure and civilians. Russian propagandists have also continued to make open threats to use [nuclear weapons](#), although there have been no concrete moves to do so, and reports suggest that [President Xi warned Putin](#) against such a course of action when they met in March 2023. However, as the year has progressed, Russian relations with China have remained close, and Russia has received substantial support with [drone technology](#) and [munition supplies](#) from Iran and North Korea, respectively.

But despite Russian resilience, the war has not gone Putin’s way. Few substantial advances have been made on the battlefield, and numerous incidents of Russian desertions have been reported. Putin also faced the highly destabilizing experience of a rebellion in June 2023, led by former ally [Yevgeny Prigozhin](#), the head of the [Wagner Group](#), a private military company. While the revolt was

defused – and Prigozhin himself died in a mysterious [plane crash](#) in August – Putin’s initially indecisive response has suggested that the foundations of his regime might not be as firm as previously supposed.

Russia’s problems have also included a resolute response from the Ukrainians, who launched a moderately successful counter-offensive against Russian positions in the south and east of the country from June into the early autumn. Throughout the year, the Ukrainians have also steadily received supplies of more sophisticated – and more offensive – US and other Western weapons, such as contingents of the [M1A1 Abrams main battle tank](#), [long-range ATACMS missiles](#), and [F-16 fighter jets](#). President Putin is also now aware that even if he were to partly withdraw from Ukraine, there is no easy way out.

Sanctions are unlikely to be lifted until Russian forces are out of most Ukrainian territory and Ukrainian reconstruction is underway.

Putin himself also faces an arrest warrant issued by the International Criminal Court (ICC) in March 2023, which held him responsible for the illegal deportation and mistreatment of Ukrainian children.

At the same time, President Volodymyr Zelensky and the Ukrainian military have faced a tough year. Blunting Russian success has not meant great advances for Ukraine, and Russian attacks on civilian life and critical national infrastructure have created much distress and hardship, even if the country as a whole remains determined to fight on. Ukraine has also been stung at times by a perception that its counter-offensive has failed because it did not make spectacular gains. There have been increasing concerns in Kyiv that the US and its allies have started to lose interest in the war – distracted by other international issues such as Gaza – and become tired of Ukrainian refusals to consider compromise. With both sides determined to keep fighting and their allies prepared to keep supporting them, the war largely achieved something like a ‘steady state’ in 2023.



The Sanctions Regime Against Russia

As we outlined in our report last year, the multilateral Western sanctions regime implemented following the Russian invasion of Ukraine has been one of the most sustained and wide-ranging applied on an aggressor since the end of the Second World War. The invasion led to an unprecedented range of international action outside the UNSC, with the [US](#) imposing further measures to an already extensive Russian sanctions framework, joined by the [EU](#), [Norway](#), [Switzerland](#), [Iceland](#), the [UK](#), [Canada](#), [Australia](#), and [New Zealand](#), [Japan](#), [South Korea](#), [Singapore](#), and [Taiwan](#). Although not all of these countries' sanctions regimes against Russia are identical, there has been a high level of coordination and complementarity between them to ensure a magnified effect. Key measures include:

- **Personal Sanctions:** These include personal asset freezes and travel bans on the Russian political elite, including President Putin and Foreign Minister [Sergei Lavrov](#), members of the Duma, Russia's parliament, military leaders involved in the invasion, regime-supporting oligarchs and business leaders such as [Roman Abramovich](#), local politicians, propagandists and soldiers and others responsible for atrocities in Ukraine.
- **Financial Sanctions:** These include asset freezes and transactional bans on Russia's official financial sector, including the Central Bank of Russia. Several major Russian financial institutions, including its largest commercial bank, [Sberbank](#), were removed from the [SWIFT](#) messaging system, which supports international financial transactions and trade. The crypto asset sector has also been affected, with the EU banning cross-border cryptocurrency transactions with Russian individuals and entities outside the EU in October 2022.
- **Sectoral Sanctions:** These have included a variety of export and import controls on strategic Russian industries and firms involved in the production or procurement of weapons, dual-use goods (e.g., drones), advanced technology (e.g., quantum computers and advanced semiconductors), iron and steel, logistics and transport, and - most controversially - Russia's massive oil and gas industry. This has included an adjustable price cap on the purchase of Russian seaborne oil products, introduced in December 2022.

Alongside these measures, the sanctioning countries have also created mechanisms for more effective sanction implementation, including a [Russian Elites, Proxies, and Oligarchs \(REPO\) Task Force](#) bringing together the efforts of the [Group of Seven](#) (G7) leading industrialized countries, the EU and Australia to identify and freeze sanctioned Russian assets.



Assessing Effectiveness

A major element of the Western sanctions effort in 2023 has been to assess effectiveness and identify potential 'course corrections.' From the macro-level, it has been hard to deny that the sanctions have failed to achieve their goals so far. The Russian army remains in Ukraine, able to fight and defend its positions against Ukrainian assaults. Its collapse does not appear imminent. In parallel, the Russian economy and key industries appear to have been remarkably resilient in the face of Western measures. While Russia has undeniably suffered, it has sustained its exports to new customers beyond its old clients in the West. Despite a year-on-year fall in [oil and gas revenues](#) of 26 percent for the first ten months of the year, official Russian figures showed hydrocarbon revenues more than [doubled](#) between September and October 2023. Russia has also managed to continue to source many prohibited imports, such as [semiconductors](#) and [vehicle parts](#), as well as weapons and munitions. An analysis by the International Monetary Fund in July 2023 assessed that the [Russian economy](#) would grow by around 2.2 percent in 2023 and by a further 1.3 percent in 2024, which, while modest, were comparable to many developed countries not currently fighting a major war.

The most pressing question for Western governments has thus been: How is Russia managing to mitigate the effect of sanctions?

Part of the problem remains delayed implementation of measures – once announced, they can take many months to put in place, allowing Russia to maximize income in the meantime. For example, Russian diesel fuel exports to Europe surged in January 2023 before an EU ban took effect in February. Legal requirements have also required previously agreed contracts to be completed, especially in the commodities trade. Some Western businesses have also been sluggish in their efforts to identify risks and vulnerabilities. According to a [report](#) in June 2023, the De Nederlandsche Bank (DNB), the central bank of the Netherlands, had found that roughly a third of financial institutions in the Netherlands had failed to track down and freeze relevant Russian assets.

The Russians have also been extremely agile and determined in finding ways to try and work around sanctions, taking some [guidance and advice](#) from long-sanctioned Iran. Key approaches have included:

- **Finding New Markets:** Russia has found an [expanding market](#) for its hydrocarbons, other commodities, and manufactures in major Asian economies such as China, India, and Turkey, with the management of these trades moving from established businesses in Western jurisdictions to pop-up traders and logistics firms in 'neutral' hubs such as the [United Arab Emirates \(UAE\)](#). While many of these commodities are being used domestically by the importing countries, there is also substantial evidence suggesting that Russian materials are mixed in with third-party commodities or simply rebadged and then resold to Western countries in breach of the restrictions. According to a report by [The Financial Times](#) in July 2023, around 90 percent of Russian oil purchased by UAE-based firms never arrived in the Emirates but went directly to buyers in Asia, Africa, and South America. Much of this trade has been transported by 'ghost fleet' container ships using techniques such as reflagging, at-sea ship-to-ship transfers, and turning off tracking devices to hide their activities.
- **Importing from Other Sanctioned States:** As noted above, Russia has worked closely with other sanctioned states, such as Iran and North Korea, to source military items such as drone technology, artillery shells, and clothing. Some reports have suggested that Russia has sought to 'buy back' its previous military exports from not only other isolated countries such as Myanmar but also neutral jurisdictions such as India, according to an analysis by [Nikkei](#).



- **Transshipment via Neutral States:** Neutral or third-party countries also play a major role in Russia's sourcing of prohibited items, as highlighted by a [joint statement](#) from the US departments of Justice, Treasury, and Commerce in March 2023. Working closely with expatriate Russian nationals and third-party nationals based in China, UAE, Turkey, and the states of the Former Soviet Union (FSU), Russian agencies and businesses have developed schemes using overseas shell companies and faked documentation to purchase and then tranship goods to Russia. According to an analysis by [The Financial Times](#) in May 2023, more than \$1 billion of restricted EU exports had never arrived at their supposed destinations in states neighboring Russia.

Alongside these sectoral measures, Russian oligarchs have also faced challenges due to Western restrictions. There is no doubt that they have generated pain. According to an analysis by [Bloomberg](#) in January 2023, Russian oligarchs lost almost \$95 billion in 2022, at a rate of around \$330 million a day. However, it now appears that many powerful Russian oligarchs targeted by individual sanctions took evasive action to blunt the worst effects of sanctions, either before they were imposed or came into effect. As a December 2022 report by the US Treasury's [Financial Crimes Enforcement Network \(FinCEN\)](#) noted, many Russian oligarchs started to restructure the ownership of their assets and make financial preparations in December 2021 and January/February 2022, in advance of the invasion. One such oligarch was Roman Abramovich, who began setting up offshore trusts for his seven children in early February.

Since the start of the war, oligarchs have continued to try and obfuscate the beneficial ownership of funds, using third parties and professional enablers based in Cyprus, the UAE, and offshore jurisdictions to place them in more opaque investments such as commercial property purchases - even in the US - managed through shell companies and pooled ownership schemes. Oligarchs, their family members, and associates have also resorted to the courts in the EU, UK, Canada, and Australia in [unprecedented numbers](#) - so-called 'lawfare' - to seek the removal of sanctions. So far, however, the results have been mixed. A handful of individuals - for example, the [mother of Yevgeny Prigozhin](#) and several [Russian businessmen](#) - have managed to have sanctions either overturned or discontinued. Still, for the majority, sanctions remain in place, and test cases such as that mounted by Abramovich associate [Eugene Shvidler](#) in the UK courts came to nothing.

Western Responses in 2023

Confronted by Russian resilience and agility, Western countries have also made their own countermoves in 2023. The [US](#), [EU](#), [UK](#), and others have added various new designations in pre-existing areas of activity, such as:

- **Russian financial institutions**, for example, new EU measures against Alfa-Bank, Tinkoff Bank, and Rosbank.
- **Russian officials and military officers** involved in the Ukrainian occupation, deportation of Ukrainian children, the management of bogus referenda in Eastern Ukraine, and the persecution of domestic dissidents such as [Vladimir Kara-Murza](#), who was sentenced to 25 years in prison in April 2023 for treason and spreading disinformation.
- **Pro-Russian propagandists and media outlets** such as RT Balkan, Oriental Review, Tsargrad, New Eastern Outlook, and Katehon.
- **Metals and mining firms**, with a particular focus on those involved in rare earth mineral extraction.
- **Transportation and logistics firms**, including firms involved in sanctions evasion and the theft of Ukrainian grain.
- **Professional services providers**, such as commercial legal support for Russian businesses.
- **Energy extraction capabilities**, such as research institutes, drilling and mining companies, and firms that broker investment in the Russian energy industry.
- **The export of electronic components**, dual-use goods, and technology that can be used in weapons systems.

A further area of renewed Western activity has been against the Russian regime's proxy mercenary group, Wagner. Having previously sanctioned the group and its senior leadership, Western countries took a range of measures in 2023, including its designation as a [transnational criminal organization](#) by the US in January and its proscription as a [terrorist group](#) by the UK in September. The [US](#) and [UK](#) have also announced a succession of sanctions against Wagner-linked groups and individuals operating in sub-Saharan African jurisdictions such as Mali, the Central African Republic, and Sudan in response to their alleged involvement in illicit gold trading, sanctions evasion, war crimes, and human rights abuses.



Tackling Evasion

While working on widening and deepening their existing sanctions regimes, Western countries have applied 'soft power' to try and improve effectiveness. The [US](#), [EU](#), and other governments' agencies have issued advisory notes to private industry to help identify evasion risks and increase effective implementation, especially with regard to export-controlled goods ostensibly being sold to third-party countries near Russia. The US has also used [diplomacy](#) to encourage neutral countries to support Western measures.

But Western countries have also taken tougher actions. At home, US authorities have arrested and charged US nationals for involvement in sanctions evasion schemes, including efforts to protect the US-based assets of sanctioned oligarchs such as [Viktor Vekselberg](#) and to [supply advanced US technology](#) to the Russian military. Private sector firms, including several in [financial services](#), have also been allegedly targeted for investigation for potential Russian sanctions compliance failures by US and European authorities. In August 2023, an [unnamed UK business reached](#) a £1 million settlement with the UK government following an investigation that had revealed unlicensed trade of goods to Russia.

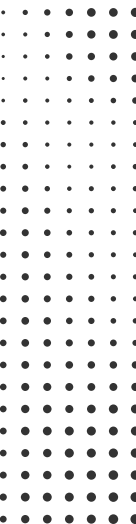
Furthermore, the US has taken the lead in using secondary sanctions against third-party nationals, businesses, and government agencies that have helped support the Russian military enterprise. [Drone technology providers in Iran](#) have been major targets, as have international 'entrepreneurs' who have sought to make profits out of the war. They include Russian nationals such as Cyprus-based arms dealer [Igor Zimenkov](#), but also third-party nationals who have been helping Russia source prohibited technology and military and dual-use goods, such as:

- [Ashot Mkrtychev](#) (a Slovakian national), who has played a key role in the management of North Korean arms sales to Russia.
- [Walter Moretti](#) (a Swiss-Italian national), has sourced sensitive US military technology for Russia through a procurement network in eastern Europe.
- [Anselm Oskar Schmucki](#) (a Swiss national) is alleged to have helped support the illicit financing of sanctions evasion.

The US, UK, and others have also targeted third-party professional enablers who have provided support for oligarchs' evasion efforts, including the Cypriot lawyers [Demetris Ioannides](#) and Christodoulos Vassiliades, who have provided services to Roman Abramovich and [Alisher Usmanov](#), respectively. The US has also increasingly taken aim at logistical firms in the Middle East that have helped ship Russian oil priced [above the price cap](#). US Treasury Secretary [Janet Yellen](#) promised more actions of this type in the future.

In comparison, the EU – which has historically not applied secondary measures – has found it more difficult to tackle evasion. However, the war in Ukraine has seen a marked shift in its approach, with the EU joining in the designation of Iranian entities involved in the [supply of drone technology](#) to Russia. Moreover, in its [11th package of measures](#), issued in June 2023, the EU also prohibited access to European ports for oil-carrying vessels where authorities had reason to believe that techniques such as transponder switch-offs and ship-to-ship transfers had been used.

However, so far, the EU has stood back from taking stronger secondary measures, deciding instead to offer technical assistance to third countries through which Russia circumvented sanctions. However, the EU also clarified that it would consider [applying export restrictions](#) to third countries that were consistently unwilling to cooperate.



Compensation and Asset Seizure

A further area where Western countries have increased pressure against Russia has been by linking sanctions relief and the use of Russian assets for the reconstruction of Ukraine. In the May [G7 meeting](#), leaders agreed that Russia's sovereign assets needed to be fully mapped and could potentially be used to pay for Ukrainian reconstruction. In June 2023, moreover, the UK announced [legislation](#) to ensure that sanctions would remain against Russia until it had paid compensation to Ukraine for damage caused and provided new options for sanctioned individuals to donate frozen funds to reconstruction efforts.

In addition, Western countries have taken more aggressive measures to use some Russian assets now rather than waiting for future compensation to Ukraine. In October 2023, EU leaders agreed that the [income generated from frozen Russian state assets](#) could be used to support Ukrainian reconstruction, and discussions have been ongoing about eventually deducting the cost of damage done to Ukraine from frozen Russian national assets. Nonetheless, some governments and financial institutions have expressed concerns about how such measures might affect international financial stability.

This effort to move from 'freezing' to 'seizing' has been a major area of discussion amongst Western governments, not only with regard to Russian state assets, but those of sanctioned oligarchs too. Here, alongside the moral question of Ukrainian reconstruction, there have been practical challenges encouraging action. While financial assets have proven easy to freeze and maintain at no cost, physical assets – properties, yachts, etc. – have not, causing practical

and financial headaches for governments. In March 2023, for example, Italian police in Trieste took possession of the [world's largest sailing yacht](#), owned by Andrey Melnichenko. With Melnichenko refusing to acknowledge ownership, however, the Italian government has been forced to support the running costs of the vessel, which are estimated to run at around 10 percent of its \$580 million value annually.

These imperatives have led Western governments to look for ways around some of the legal challenges of seizing the assets of private individuals as reparation for their home state's international aggression. The US has been at the forefront of efforts to creatively apply [existing laws](#) on criminal seizure. In December 2022, President Biden signed a [law](#) allowing the US Department of Justice to seize some frozen private assets and transfer them to the Department of State to support Ukrainian reconstruction. In February 2023, this power was used for the first time when a New York federal district judge agreed to prosecutors seizing \$5.4 million from Russian oligarch [Konstantin Malofeyev](#), which could then be used in reconstruction efforts. Nonetheless, progress on 'freeze and seize' has been relatively slow, and some jurisdictions have halted completely. In [Switzerland](#), – which holds a huge amount of designated private Russian wealth – the Federal Office of Justice (FOJ) concluded in February 2023 that the confiscation of private Russian assets for reconstruction purposes was prohibited under the Swiss constitution. Although other governments remain focused on pushing forward, few are under any illusion about how difficult it will be without major legal changes.





2024 Prospects

Predicting the course of the war in 2024 is hard, as such attritional conflicts have a tendency to remain stable for long periods before breakthroughs occur due to one side's collapse or exhaustion. Given the balance of forces, it is likely that the war will continue within its current parameters, with further Russian offensive and Ukrainian counter-offensives in the spring and summer. Given the increasing accumulation of high-quality Western equipment on the battlefield, there is an opportunity for Ukraine to make greater progress than it did in 2023 – however, the Russians remain heavily dug-in, and the Ukrainians are low on manpower.

The most substantial developments are likely to come off the battlefield, as Western countries will pressure Ukraine to start looking to some form of negotiation.

Changing domestic political environments have started to have an effect – [Western publics' attentions](#) increasingly shifting attention elsewhere – and the prospects of changing political leadership in the West have raised questions about the level of Western commitment to Ukraine in the long term. Indeed, it seems likely that European efforts to find a way to end the conflict on grounds relatively favorable to Ukraine will accelerate if it looks likely that Donald Trump – no great friend to Ukraine – will be re-elected as US President in November.

Pressure to make a deal might also be brought to bear on Putin from both domestic allies and President Xi. It is notable how careful China has been not to aggravate the US by providing overt military support to Russia. However, there is evidence of some material being supplied through [back channels](#), despite Xi's promise of a "no limits partnership" in 2022. Chinese circumspection about the conflict has started to exhibit itself in various practical ways, with the [Bank of China](#) deciding in the summer of 2023 to restrict Russian bank clients transacting with various Western banks and starting to terminate Russian transactions in Chinese yuan, US dollars, Hong Kong dollars, and euros, through correspondent accounts.

However, even if talks begin, progress is likely to be slow and tortuous, given the level of enmity between both sides. This suggests that any material reduction in Western sanctions against Russia will be extremely unlikely in 2024, and what we are more likely to see is:

- The introduction of a small number of **new sectoral bans**.
- More **loopholes closed** in existing sanctions, crackdowns on evasion, and poor compliance, with large fines and settlements likely.
- More targeting of **third-party nationals and businesses** aiding the Russians in circumventing sanctions in the sale of oil above the price cap and sourcing of high technology goods, especially in jurisdictions such as UAE, Hong Kong, and Turkey.
- Efforts to energize **freezing and confiscation** efforts, perhaps through the support of proposals for lawyers to become 'privateers' in identifying and freezing Russian assets, allowing them a cut of any eventual seizures.

In response, Russia has limited scope for retaliatory economic and financial counter-measures, as Western countries have largely cut themselves off from those trades with Russia that were most important to both sides, especially in hydrocarbons. Russia has thus been relatively half-hearted in its application of sanctions against Western countries, with a smattering of sectoral bans and individual sanctions against perceived anti-Russian sentiment. In March 2023, for instance, Russia imposed sanctions on [23 UK citizens](#), including military officers, judges, and political commentators and analysts. Russia has also sought to encourage criminal activity against Western interests, such as by raising bans on [luxury counterfeit goods](#) being manufactured in and transiting through the country.

Nevertheless, these actions are minor, and Russia is much more likely to focus its energies on developing more complex and intricate schemes to continue trading, as has been seen before by Iran and North Korea. For Western countries, therefore, targeting third-party intermediaries will become a 'whack a mole' process, as newly minted front companies are set up to replace recent designations. Russia's potential for success in making this work will thus come down to the willingness of neutrals amongst Russia's neighbors, in the Middle East, India, and China, to turn a blind eye and take only nominal measures to placate the US and other Western countries. Up to now, that seems to have been the approach of many neutrals. It is likely to remain so – to Russia's benefit – unless the West makes the decision to risk losing some friends and potentially make some new enemies.



What does this mean for my firm?

“ Businesses with clients in high net worth and PEP categories need to have the best data available to identify their potential exposure to Russian oligarchs, their families, associates, and commercial interests. Public registries need to be supplemented with the very best available commercial data. In our State of Financial Crime 2024, 73 percent of firms said they would need to reduce their reliance on manual PEP screening processes in the year ahead. This indicates many firms have urgent and important technology investments to make.

Businesses with exposure to key sanctioned sectors such as hydrocarbons, metals and mining (especially gold), technology, and dual-use goods need to ensure their screening and transaction monitoring platforms cover neutral jurisdictions of operation with known links to Russia take into account information from guidance from bodies such as the US Treasury’s Office of Foreign Assets Control (OFAC) and FinCEN.

Businesses need to think seriously about taking a proactive response to risk management and reaching out to appropriate authorities early if they identify areas of concern. ”



Andrew Davies

Global Head of Regulatory Affairs,
ComplyAdvantage

The US Sanctions Regime

Outside of the UNSC regime, the most widely recognized sanctions regime is that of the US, which is enforced primarily by the Department of Treasury's Office of Foreign Assets Control (OFAC). The designations of entities and individuals are made under country-specific or thematic regimes, legally underpinned by legislation or Presidential Executive Orders (EOs). Beyond OFAC, the US Commerce Department's Bureau of Industry and Security (BIS) plays a growing role, managing lists of foreign firms subject to export controls (the most significant being the Entity List). Unlike other sanctions regimes, which apply only to those subject to the legal authority of the sanctioning authority, US law also allows the government to impose sanctions on non-US citizens and entities engaging in specified activities with designated targets (known as primary and secondary sanctions, respectively).



Major Hotspots: Iran

The Islamic Republic of Iran has been subject to a variety of Western sanctions since the Islamic Revolution of 1979. The primary sanctioning state has been the [US](#), which has applied stringent sanctions against Iranian hostage taking, overseas interference by the [Iranian Revolutionary Guard Corps \(IRGC\)](#), support for Islamist extremist groups such as [Hezbollah](#) and [Hamas](#), human rights abuses at home, cyber criminality, and Iran's attempts to develop military nuclear technology and ballistic missiles.

With regard to the Iranian development of nuclear weapons, the US has managed to coordinate some action with other states and international organizations, such as the UNSC and EU, over the last two decades, with the removal of Iranian financial institutions from the [SWIFT](#) financial messaging system in March 2012, and a [ban](#) on the import of Iran's primary exports of oil, gas, and other hydrocarbons. This coordinated pressure led to the signing of the [Joint Comprehensive Plan of Action \(JCPOA\)](#) in July 2015 between Iran, the members of the UNSC, Germany, and the EU, which allowed Iran partial access to the international financial system and global commodity markets in return for limits on uranium enrichment.

However, the [Trump administration](#) withdrew the US from the JCPOA in May 2018, citing Iranian breaches and malign interference in neighboring countries such as Iraq, and reimposed sanctions later that year. Despite efforts to revive US participation in the deal by Trump's successor, [Joe Biden](#), talks brokered by the [International Atomic Energy Authority \(IAEA\)](#) produced only limited progress and no concrete outcome by the end of 2022. The failure resulted from [disagreements](#) over the terms of the deal but also partly from friction over Iran's support for Russia in Ukraine and its violent crackdown against Iranians protesting against the death in custody of [Mahsa Amini](#) in September 2022. As noted in last year's report, both of these Iranian acts led to successive rounds of coordinated Western sanctions against Iranian individuals and businesses involved in exporting drone technology to Russia and law enforcement and judicial officials involved in human rights abuses.

2023: Hopes Denied

The atmosphere of Iranian-Western relations changed very little in 2023, although there were some reasons for cautious optimism. In August, the US agreed to transfer [\\$6 billion](#) from Iranian oil sales, frozen in an account in South Korea, to a Qatar-based account where they could be used for humanitarian purposes in Iran. The following month, Iran released five US nationals held in its custody. In November, the US also extended a [waiver](#) to allow Iraq to pay Iran for electricity supplies.

Nonetheless, these small developments did not amount to a major strategic change, and

the general tenor of relations between Western countries and Iran has remained frosty.

Western countries expressed grave concerns about the [IAEA's report](#) in early 2023 that Iranian uranium enrichment had reached nearly 84 percent (90 percent enrichment being 'weapons grade'). Official talks between the US and Iran did not progress. However, indirect discussions under [Omani auspices](#) over the summer generated some goodwill, which contributed to the agreement of the prisoner exchange deal. But at the same time, the US and others continued to take issue with Iran's military support for Russia, its sustained repression of dissidents at home, and its support for militias in Iraq, Syria, and Yemen. Following the Hamas attacks on Israel on October 7, the US also [warned](#) Iran – a significant

financial and political backer of the terrorist group – not to intervene either directly or indirectly through its Lebanon-based ally, Hezbollah.

Western countries thus elected to sustain sanctions against Iran throughout 2023. In the autumn, the EU, France, Germany, and the UK announced that they would [maintain nuclear sanctions](#) against Iran that had been set to expire on October 18 under the JCPOA, incorporating measures such as prohibiting the export of ballistic missile technology into their own sanctions frameworks. In addition, Western countries focused on applying tougher measures to Iranian sanctions evasion, overseas interference, and repression at home:

- **Targeting Iran's shadow banking and logistics networks:** In 2023, the US continued to target the growing [web of front companies](#) in Hong Kong, South East Asia, and UAE being used to organize illicit Iranian oil sales by the Persian Gulf Petrochemical Industry Commercial Co. (PGPICC) and Triliance Petrochemical Co. Ltd. (Triliance). In July 2023, the US also banned [14 Iraqi banks](#) from transacting in US dollars over fears that Iran was using these banks to support its commercial, financial, and military activities. Closer to come, the US continued to pursue those it alleged to be supporting Iranian procurement and illicit financing, such as Salim and [Khalil Henareh](#), who were indicted in February 2023 for laundering millions of Iranian oil dollars through Canadian money service businesses and front companies.
- **Targeting the IRGC:** [Calls](#) mounted in the EU, UK, Canada, and Australia to proscribe the IRGC as a terrorist organization, as is already the case in the US. So far, these governments have resisted these demands but have also moved to target the [IRGC](#), IRGC leaders and officials, and linked businesses, charities, and investments for involvement in domestic repression and illicit financial schemes.
- **Targeting Drone Technology:** As noted in the previous section, the US, EU, UK, and others have continued to designate Iranian officials, military officers, businessmen, government organizations, and businesses linked to the [supply of drones](#) and drone technology to support the Russian war effort in Ukraine.

- **Targeting the Iranian Parliament, Law Enforcement, and Judiciary:** Western countries have widened the scope of personal sanctions against Iranian officials and parliamentary representatives involved in the persecution of domestic protesters and the use of the death penalty to silence dissent, notably the UK's designation of Prosecutor General Mohammad [Jafar Montazeri](#) and his deputy [Ahmad Fazelian](#) for the execution of UK-Iranian national [Alireza Akbari](#) in January 2023.

In the face of tightening Western measures, Iran has sought to bolster its struggling economy and reduce its isolation by moving closer to countries opposed to the Western rules-based order, especially Russia and Venezuela, but also China, as well as neutral states such as India and South Africa. Iranian efforts have been largely welcomed, moreover, with the country joining the [Shanghai Cooperation Organization \(SCO\)](#) in July, an economic and security group led by Russia and China, and invited to join the [BRICS](#) group (Brazil, Russia, India, China, and South Africa) of emerging economies in August. Nonetheless, neither of these groups can be seen as 'alliances' as such. Despite growing oil sales, the immediate positive impact on the Iranian economy seems to have been small, at least for now.

2024 Prospects

With the US presidential election coming – and a Trump/Biden rematch in prospect – it seems improbable that the current administration will seek to take any major political risks over Iran, especially given the wider context of Iranian conduct and the instability in the Middle East. Joe Biden will not want Trump to be able to label him as 'soft on Iran.' It seems likely that the EU, UK, Canada, and others will also increasingly cleave towards the US position on Iran, especially with sanctions of overseas IRGC activity and human rights abuses. Given the known links between Iran and Hamas, there is likely to be an effort to identify and designate more parts of the financial and procurement chain between the two, as well as suppliers and intermediaries in Iran's drone trade with Russia.

However, it also seems unlikely that there will be a large-scale escalation in Western sanctions, partly because of the limited opportunities available to do so. But also because Iran, despite remaining obdurate in the face of

Western pressure, seems [cautious](#) about pushing the US too far over the Israel/Gaza conflict. Despite rhetorical and financial support for Hamas, Iran has been careful not to weigh in to the conflict too overtly. This, of course, could change, especially if fighting widens to southern Lebanon and Syria, prompting a more open role as the backer of anti-Israeli forces. This would likely produce a firm response from the US, EU, and UK, with new designations and more secondary measures against third parties dealing with Iran. Increased domestic repression or overseas interference could also prompt such moves. But the balance of probabilities suggests 'more of the same' for the West and Iran in 2024. The real prospect for radical change will come in 2025, depending on the outcomes of a range of variables such as the US presidential election, the progress of the war in Ukraine, and the state of US relations with China.

What does this mean for my firm?

As with Russia, businesses with exposure to third-party neutral jurisdictions and sanctioned sectors – especially hydrocarbons – will need to ensure they have the best risk data available, combined with agile and configurable screening platforms, to take account of the US's attempts to keep up with the sophistication of Iranian sanctions evasion techniques.

Businesses with exposure to Middle Eastern jurisdictions will need to give particular attention to ensuring that they have appropriate coverage of risks from client links to IRGC business concerns and proxies, especially in sectors where the IRGC is known to have major interests, such as construction.

Businesses with potential exposure to Russia and Iran – and with jurisdictions with known commercial and financial links to both – will need to ensure that policies and controls are in place that might identify any sanctioned trades taking place between the two, especially regarding dual-use technologies.



Iain Armstrong

Regulatory Affairs Practice Lead,
ComplyAdvantage



Major Hotspots: North Korea

North Korea (officially the Democratic People's Republic of Korea, or DPRK) has continued to pose a major problem for the international community, with its defiant pursuit of nuclear weapons and ballistic missiles, domestic repression, various illicit activities, and more recently, its active support for Russia's invasion of Ukraine. Besides these challenges, the regime of Kim Jong-un also has the potential to collapse at any time. Despite a defiant stance toward the outside world, North Korea has struggled to keep its siege economy afloat, hampered as it has been by inefficiency, corruption, the trauma of COVID, and the long-term effect of sanctions.

The initial and primary source of sanctions has been the US, targeting North Korea's involvement in conventional weapons proliferation, terrorism, drugs trafficking, counterfeiting, smuggling, money laundering, human rights abuses, Weapons of Mass Destruction (WMD) development, and latterly cybercrime. North Korea faces among the most comprehensive packages of US sanctions, with bans on all trade apart from food and humanitarian goods, asset freezes, transactional bans, and the personal designation of many regime officials. Since the 1990s, other members of the international community have also aligned with the US over the North Korean nuclear program. Following Pyongyang's first successful nuclear test in October 2006, the UNSC began imposing rounds of ever tighter sanctions. More recently, as Russia and China have stymied efforts to impose further restrictions via the UN, several Western or Western-oriented organizations and countries, including the EU, the UK, Canada, Japan, South Korea, and Australia, have introduced their own national sanctions against North Korea, with a particular focus on nuclear weapons proliferation.

2023: Dangerous Friends

There have been few glimmers of hope for improving North Korea's relationship with the US and others in 2023. Some minor areas of cooperation have emerged, such as North Korea's return of US serviceman Travis King in September, two months after he had strayed across the Demilitarized Zone (DMZ) separating the two Koreas.

But at a strategic level, there has been sustained hostility, with North Korea growing closer to Russia throughout the year. While there were suspicions of North Korea supplying Russia with munitions in 2022, these were largely confirmed during 2023, with the scale of transfers increasing as the year progressed. In March, the UN Panel of Experts on North Korea further confirmed that Russia had resumed oil sales to North Korea at the end of 2022, with volumes rising over time. North Korea and Russia also undertook an intense round of diplomacy over a more comprehensive military and economic deal, with Russian defense minister Sergei Shoigu visiting Pyongyang in July and the North Korean leader Kim Jong-un journeying to Russia to meet President Putin in September. There were also discussions of joint Russian and North Korean naval drills and the sharing of military satellite technology. By the fall of 2023, however, no new deal had been announced. Some Western commentators speculated that both Russia and North Korea were looking for China's blessing for such an open breach of UNSC restrictions.

As North Korea deepened its ties with Russia, it continued to provoke its near neighbors and the US with aggressive military activity. At the end of 2022, Pyongyang mounted a drone intrusion into South Korean airspace and launched numerous ballistic missile tests, including the firing of a long-range missile toward Japan in July and two failed military satellite launches. North Korean threats to increase nuclear weapons "exponentially" and to shoot down US spy planes added to the tension. In the background, North Korea continued to secure prohibited military goods to support its prohibited weapons programs, with a major independent investigation by The Financial Times and the Royal United Services Institute (RUSI) in London showing close collaboration between the Chinese Triads in the organization of ship-to-ship transfers of illicit goods. In addition, the North Koreans maintained their wide range of illicit initiatives to generate hard currency, especially through the theft of cryptocurrency. In January, the FBI stated publicly that the North Korean hackers the Lazarus Group had stolen \$100 million in crypto from the Horizon Bridge crypto trading service in 2022, and in its March report, the UN Panel of Experts noted that North Korean hackers had stolen more crypto in 2022 than in any previous year, and double the amount from 2021.



The Western Response

The US, EU, Japan, Australia, and other states have made explicit warnings to North Korea about the potential consequences of its ongoing recalcitrance, provocative behavior, and growing relationship with Russia. [South Korea](#) has openly discussed developing its own nuclear weapons in response to North Korean activity, as well as potentially [donating arms](#) to Ukraine directly rather than its current indirect approach of filling the gaps in US stockpiles arising from supplying Ukraine. The US, Japan, and South Korea, who held a [trilateral summit](#) in August, have also begun to explore closer trilateral security links to contain North Korea. Alongside these diplomatic moves, the US – supported on different occasions by Japan and South Korea – has imposed various further designations to combat North Korean illicit and aggressive actions in the following areas:

- **Targeting weapons sales:** As noted above, the US has targeted third-party nationals such as Ashot Mkrtychev, as well as [North Korean nationals](#) based in Russia, who have been designated for the organization of North Korean munition sales.
- **Targeting weapons procurement:** The US has listed North Korean nationals linked to the country's [Second Academy of Natural Sciences](#) but operating in China for efforts to source ballistic weapons technology. The US alleges these individuals are part of a wider procurement network with elements in China and Iran.
- **Targeting currency generation:** The US has identified and designated ongoing North Korean [commercial activity](#) in Africa and the Middle East prohibited under UNSC resolutions, with North Korean companies and nationals providing prohibited construction and art services for foreign currency. The US also designated a Russian national, businessman [Sergei Kozlov](#), who has been listed for using North Korean workers in construction projects.
- **Targeting cybercrime:** The US made an additional designation linked to its previous listing of the cryptocurrency mixer [Tornado Cash](#) in 2022, with the listing of one of Tornado Cash's founders, Russian national [Roman Semenov](#), for helping North Korea launder its crypto thefts. The US also designated the [Pyongyang University of Automation Technical Reconnaissance Bureau](#) and its 110th Research Center – believed to be a cybercrime group. South Korea sanctioned the North Korean state-sponsored group '[Kimsuky](#)', which uses email phishing techniques to steal military secrets.

The US has also taken law enforcement action to close down North Korean activities within its border. In January, [Mun Chol Myong](#), the first North Korean national to be extradited to the US, detained originally by Malaysian authorities, was sentenced to 45 months for sanctions evasion and money laundering on behalf of the regime. However, this was taken as time served, and he was immediately deported home. The US also indicted [North Korean](#) and third-party nationals involved in cryptocurrency laundering, including two of Tornado Cash's founders – the aforementioned [Semenov](#) and [Roman Storm](#). Storm – a US citizen living in Washington state – was also arrested in August. Finally, in an unprecedented move in October, the FBI seized \$1.5 million and 17 domain names from unnamed US companies that had illegally paid [North Korean IT contractors](#) based in Russia, China, and other jurisdictions. The FBI stated that as a result, the contractors had been able to send millions of US dollars back home over several years.

2024 Prospects

North Korean behavior – aggressive and provocative though it is – has become predictable over the last thirty years. There can be little doubt that the regime in Pyongyang will persist in its pattern of defiance and confrontation, emboldened as it will by growing ties to Russia. There is always the risk, therefore, that North Korea will go a step too far, firing a ballistic missile through Japanese airspace, downing a Western surveillance flight, or conducting a new nuclear test. The emergence of a more comprehensive military and economic cooperation deal with Russia would also be another potential trigger for a severe response from the US – although, again, there is limited room for additional designations. More likely, such action could encourage others, such as the EU, UK, Canada, and Australia, to more closely align their approach on North Korea with that of the US, akin to how the West has dealt with Russia and Iran in recent years.

Nonetheless, Pyongyang has become an expert at dancing on the edge of provocation, and it seems probable it will avoid taking actions that would make its life more difficult than it already is. Despite its closer ties with Russia, North Korea knows there are limits to what Russia can provide as long as it continues to claim to support [UNSC sanctions](#). The main factor in what happens next will be the attitude of China. While on the one hand, providing some support for Russia,

acting as North Korea's economic lifeline, and turning a blind eye to North Korean evasion activity across its border and in its national waters, on the other, China has maintained a certain distance from both parties. China has taken exception to [Western surveillance flights](#) tracking ship-to-ship transfers off the Korean coast, sometimes responding with dangerous aerial intercepts. But it still insists that it supports the UNSC sanctions. Responding to allegations of weak sanctions implementation from the G7 and EU in July, the Chinese government insisted that it implemented UN sanctions "[strictly](#)." China will, therefore, probably not appreciate North Korea or Russia making moves that will put it in a more awkward position vis-à-vis the US. Indeed, while deeper North Korean and Russian links will potentially help China, averting a Russian defeat or a North Korean collapse, Beijing will probably not wish to be seen as too overt a supporter of the partnership for fear of Western reactions. Its circumspection is, therefore, likely to remain an ongoing brake on North Korean recklessness in 2024.

What does this mean for my firm?

Businesses with Asia-Pacific exposure, especially in the logistics sector in jurisdictions such as Singapore, will need to keep up-to-date with sanctions evasion techniques used by Pyongyang to move goods and manufactures into North Korea, especially through ship-to-ship transfers.

Financial institutions with a substantial trade client book must also pay attention to red flags in trade documentation or transactional patterns.

Businesses with exposure to sectors (such as IT firms using offshore programmers) and regions (such as Sub-Saharan Africa) in which North Korea has been known to generate hard currency through the clandestine deployment of North Korean nationals should pay particular attention to any potential red flags through the use of adverse media screening.



Alia Mahmud

Global Regulatory Affairs Practice Lead, ComplyAdvantage

Major Hotspots: China

While not a 'rogue state' like Russia, Iran, or North Korea, China, led by President Xi Jinping, is the largest and most long-term geopolitical challenge for Western countries. The People's Republic of China (PRC) not only represents a major authoritarian alternative to the Western democratic model, it does so whilst also being amongst the most economically successful economies in the world. Its GDP has grown rapidly since the 1990s and stood at around [\\$17.9 trillion in 2022](#) – second only to the US – which it is likely to [surpass](#) in the next two decades.

China – Opportunity and Challenge

While on the one hand, a positive spur for global growth, China's growing economic preponderance has also increased its economic and political weight, not only within the Asia-Pacific region, where it plays a leadership role in groups such as the Shanghai Cooperation Organization (SCO) but further afield, into the Middle East, Africa, and Europe. Primarily, this has been through its massive communications and logistical investment program, the [Belt and Road](#) (BRI) trade initiative.

While China has remained careful not to fall into alliances with other authoritarian states such as Russia, it has provided rhetorical support.



In 2022, Xi referred to a “[no limits partnership](#)” with President Putin – and economic opportunities for heavily sanctioned states like [Iran](#).

At the same time, it has become more assertive about its national security at home and abroad. China has reacted angrily to Western criticisms of its [domestic surveillance](#) measures, the mistreatment of minorities such as the [Tibetans](#), Muslim [Uyghurs of Xinjiang](#), and the [Falun Gong](#) religious sect, and the undermining of civil liberties in [Hong Kong](#), a Special Administrative Region of China with nominal control over its own internal governance. China also reacted angrily to [Australian](#) charges of a lack of openness over the outbreak of the COVID pandemic in Wuhan in early 2020, leading to the imposition of massive Chinese tariffs on major Australian exports.

Under Xi, China has become extremely assertive over territorial claims to waters and island chains in the [South](#) and [East](#) China Seas, and most importantly, its ‘[One China](#)’ policy toward the island of Taiwan. The island, to which the Chinese nationalists retreated in 1949 after defeat in the Chinese Civil War, has been autonomous from the mainland ever since and has developed into a prosperous democracy under US military guarantee. The island’s status and Western support for it have been a running sore between China and the US since the 1950s and have occasioned numerous crises and ongoing tension. In 2022, for example, there were major frictions between the US and China when then Speaker of the US House of Representatives, [Nancy Pelosi](#), visited Taiwan, and President Biden re-affirmed [US military support](#) for its independence.

A Growing Friction

Throughout most of the first decade of the 21st century, the Western response to China’s rise was positive and twin-tracked. On the one hand, it sought to make China a constructive player in the global economy while encouraging it to liberalize at home and take a conciliatory path overseas.

In the last decade, however, Western countries, led by the US, have become increasingly concerned about China’s imperviousness to Western criticism of its domestic and overseas policies and have sought to work more closely with [regional partners](#) in the Asia Pacific to balance against Chinese influence.

In addition, the US has increasingly turned to sanctions to register its displeasure, with a framework of measures that have developed under Presidents Trump and Biden that focuses on:





- Export controls to stop the Chinese military and technology sectors from accessing US technology, most notably President Biden's ban on the export of [semiconductors](#) and chip-making machinery in October 2022.
- Prohibiting the use of Chinese technology in areas of national security significance, such as [5G telecommunications infrastructure](#).
- Targeting officials, institutions, and businesses alleged to have been involved in human rights abuses, including the persecution of the [Uyghurs](#) and the suppression of civil liberties in [Hong Kong](#).

Several of the US's allies have started to follow the American lead on China in recent years, such as the [UK](#) and [Australia](#) removing the involvement of Chinese technology giant Huawei in its 5G rollouts and the [EU](#), [UK](#), and [Canada](#) sanctioning Chinese officials for complicity in internal persecution.

China's own response to these developments – apart from critical rhetoric – has included the overhaul of its sanctions regime, with the creation of an '[Unreliable Entities List](#)' (UEL) and a [Blocking Statute](#) and [Anti-Foreign Sanctions Law](#) (AFSL) to prevent companies following foreign sanctions. However, the application of the regime has been limited so far, with the Chinese preferring to target individual Western politicians and officials, such as [Nancy Pelosi](#), deemed to take an 'anti-Chinese' position.

2023: The Hot Peace

2023 has largely left the overall structure of the geopolitical relationship between China, the US, and its allies largely as it was – what [John Thornhill](#), a columnist at The Financial Times, has described as a "hot peace." Within this framework, though, the year has also seen five developing trends, some with negative portents for the future and others that give grounds for guarded optimism.

01

The first trend has been the consolidation of domestic power around President Xi after his historic appointment to a [third term](#) by the Chinese Communist Party's 20th Congress in October 2022, [confirmed](#) in March 2023. Following the end of China's '[Zero Covid](#)' policy in early January 2023, the Chinese economy has grown again, with a [5.4 percent growth rate](#) predicted in 2023 by the IMF. Xi has also sought

to re-shape his top leadership team, removing [two senior military commanders](#) in the summer over loyalty concerns and the foreign and defense ministers [Qin Gang](#) and [Li Fangshu](#) in June and September, respectively. However, with ongoing challenges from deflation, commercial debt, and a sluggish property market, domestic events have not always been in Xi's favor. Foreign Direct Investment (FDI) has also fallen throughout the year – [dropping a dramatic 34 percent in September](#) – off the back of fears that US economic and trade measures will decouple China from the global economy.

02

The second trend has been China's desire to play a global role commensurate with its political and economic strength. Much of this – while clearly designed to compete with the Western approach – is not by definition malign, such as China's promotion of the [BRICS](#) group as a potential alternative framework to the Western dominated G7 – an idea restated by Xi at the BRICS conference in South Africa in August. China has also played a positive diplomatic role in improving international relations, brokering as it did the re-establishment of diplomatic relations between [Iran and Saudi Arabia](#) in March. However, there have been negative sides to China's global diplomatic offensive, with Beijing cultivating closer ties with rogue actors such as [Iran](#), the [Taliban](#) in Afghanistan, and President [Assad](#) of Syria. Of most concern to the West, though, has been China's relationship with Russia. In March 2023, President Xi traveled to Moscow and restated China's "[deep friendship](#)" with Russia, hailing growing economic and trade ties between the country, while in July, China and Russia joined [joint naval exercises](#) in the Sea of Japan. Nonetheless, in the face of US warnings, China has avoided making large-scale contributions to the Russian war effort in Ukraine and has sought instead to play [peacemaker](#), keeping contact open with Ukraine.

03

The third trend has been China's ongoing military assertiveness in defending its perceived core national interests. In March 2023, [Xi](#) told the delegates of the National People's Congress (NPC) that they must have greater economic and technological self-reliance in the face of US and Western hostility and should "dare to fight" if need be. China has also continued to make assertive military moves in the region, launching [drills around Taiwan](#) in April and August in response to respective visits to the US by the current Taiwanese President, [Tsai Ing-wen](#), and the Vice-President and leading presidential candidate

for 2024, [Lai Ching-te](#). There were also numerous stand-offs between the [Chinese Coast Guards and Philippines supply ships](#) in the South China Sea, [near collisions](#) between Chinese military aircraft against the planes of the US and its allies, and the remarkable discovery of a [Chinese spy balloon](#) floating across the continental US in February.

04

The fourth trend has been attempted by Western countries to **resist but not provoke China**. The US and its allies in Asia-Pacific have continued to improve defense cooperation, and Western security agencies have warned about the massive scale of [Chinese commercial and political espionage](#). The Biden administration has sought to combat Chinese inroads through a sustained tough line on technology security, stopping the provision of [special licenses](#) for the export of US parts to Huawei in February, banning US private equity and venture capital [investment in Chinese AI](#), semiconductors and quantum computing businesses from 2024 in August, and [extending the semiconductor export ban](#) to cover a wider range of chips and 21 third-party destinations (including China and Iran) in October. Also, the US designated several private Chinese companies for exporting sanctioned [microchips](#) to Russia, supporting the [trade in opioid precursors](#), which has fuelled the Fentanyl epidemic in the US, and Chinese firms supporting the [Pakistan ballistic missile program](#).

However, the US government has been careful not to identify the activities of any of these companies with the Chinese government, instead [seeking Beijing's help](#) in tackling the problems. Notably, the October designation of Chinese firms for supplying microchips to Russia also included firms from India, Turkey but also Western countries such as Germany and the UK. There was no attempt to single China out. Added to this, the US has also sought to tamp down [military rhetoric](#) about a potential Chinese invasion of Taiwan, and to keep open diplomatic channels with China, with high level contacts between the two sides resuming from June onwards. As a result, Xi and Biden met in San Francisco in November 2023, making some progress on areas such as resuming its previously canceled [strategic military dialogue](#).

US allies have taken a similarly balanced approach to the US. [Japan](#) and [the Netherlands](#) – two of the world's leading microchip suppliers – also announced Chinese export restrictions in support of the US, and the EU, UK, and others began serious assessments of how they might [de-risk](#) their economies in the face of the Chinese national security challenge. [Italy](#), for example, has been reconsidering its involvement in the BRI. However, leaders such as the French

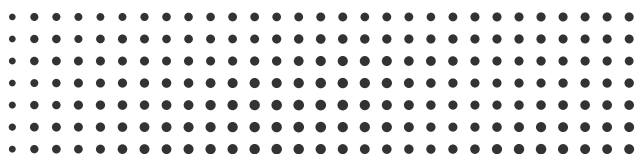
President, [Emmanuel Macron](#), who visited Beijing in April, also highlighted the importance of an ongoing economic relationship with China and the need to maintain open channels of communication. Perhaps with these concerns in mind, the EU only added a handful of Chinese firms based in Hong Kong to its [11th package](#) of Russia sanctions in June, and by the autumn, the [EU and Chinese trade representatives](#) were talking again about the need to ensure that export control issues did not undermine overall economic cooperation.

05

The fifth trend, and one that mirrors that which preceded it, has been China's own willingness to take a carefully calibrated economic response to Western actions. Admittedly, there has been significant pressure on Western firms operating in China. Chinese authorities began a national security investigation against US memory chip developer [Micron](#) in April, launched raids on US due diligence firm the [Mintz Group](#) in March, and banned [Apple iPhones](#) from government usage in September. In October, China responded to the expansion of the US chip export ban with tighter export controls on [graphite](#) – essential to the construction of batteries for electric cars. It has also met American support for Taiwan with sanctions against [US defense contractors](#) and those – including the then US House Speaker [Kevin McCarthy](#) – who supported the visit of the Taiwanese president to the US in April.

However, the most notable fact so far is how narrow and focused China's economic countermeasures have been. Despite introducing the legal framework for imposing wide-ranging sanctions against US and Western businesses over recent years, strengthened again by a new [foreign relations law](#) in June, China has not felt the need to use it extensively.

One further straw of hope in 2023 has been China's ongoing review of its tariffs against Australia, suggesting that for all its bellicosity and sympathy for anti-Western states such as Russia, China still has a strong desire to do business with the West.



Prospects for 2024

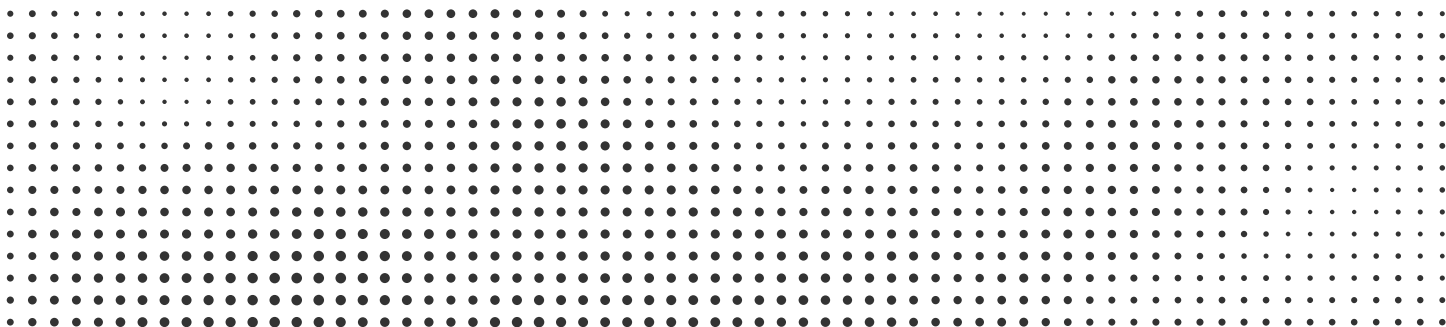
At the start of 2023, after the Chinese spy balloon debacle, it would have been a brave analyst who would suggest that by year end, Chinese-Western relations would be in a more stable condition – and yet, they are. This shows how difficult it is to take account of accidents and random contingencies, and it suggests we should be cautious about what is coming in 2024. Despite the current fair weather, several events could push in a negative direction. If the new Taiwanese President – likely to be the current VP Lai Ching-te – takes a robust approach toward China, Beijing may respond aggressively. Similarly, if Russia looks to be facing military defeat, China might feel driven to provide overt material support, which will almost certainly provoke a major Western sanctions response – even in the face of the economic anxieties of US allies in the Asia-Pacific region and Europe. This then could at last trigger a major Chinese economic counter-response, or possibly a blockade or military action against Taiwan.

But while possible, these outcomes do not look probable. Despite his very public nationalism, President Xi has much to occupy him domestically, and with the sacking of major military figures in 2023, it seems unlikely he has any intentions of ordering the People's Liberation Army (PLA) into action in 2024. And although he has no interest in seeing Russia defeated, Xi is also unlikely to see benefit in facing massive Western sanctions in order to bail out a near-defeated country. The fundamentals of the current situation suggest that for China, its economic and political interest is to maintain a mixture of challenge and collaboration towards the US and the wider West.

This stance suits Western countries well themselves, aware as they are of the potentially catastrophic consequences of China's isolation from the global economy. It is quite possible – even likely – that the US will follow through in 2024 on the designation of further Chinese firms for helping Russia evade

sanctions, as threatened by US Treasury Secretary Janet Yellen in November 2023. However, Western governments will avoid taking sweeping measures, especially against significant state-linked Chinese businesses, and frame sanctions much in the way that the US currently does with Fentanyl-related measures against Chinese firms – in other words, as measures intended to deal with unwelcome activity unconnected to the Chinese government. Despite her admonitions to the Chinese, [Yellen](#) has also emphasized repeatedly that she only seeks de-risking, and not decoupling, from China.

Whether this situation will last beyond 2024 is uncertain. The current fundamentals outlined above – Chinese domestic preoccupations and Western fears of an economic catastrophe in the event of a Taiwan crisis – are likely to sustain the current 'steady state' into the medium term. But this balance could change if, for example, the US presidential election led to the return of Trump, China's economic performance accelerated, or Russia were to win an outright victory in Ukraine. Any of these could embolden or provoke China into a more aggressive stance. Given Xi's past rhetoric, there are good reasons to believe that, eventually, China under his leadership will take action to reclaim Taiwan. China has been building up its military strength and watching Russia's difficulties in Ukraine closely to learn the lessons. It has also been taking action over recent years to prepare itself for a forced decoupling from the global economy, from the [stockpiling](#) of key commodities and goods, to the development with Russia of the [Cross-Border Interbank Payment System \(CIPS\)](#) as an alternative to SWIFT. While only currently processing a fraction of the transactions that SWIFT currently tackles, the existence of CIPS means that China – and its friends – have a trading backstop in the event of a major crisis. Although a crisis does not seem imminent, it remains possible in the medium and likely in the long term.



What does this mean for my firm?

Businesses need to fully understand their potential exposure to Chinese sectors at risk from future Western sanctions, especially those operating in the technology sector, key commodities such as hydro-carbons, as well as the chemical and pharmaceutical industries.

Businesses also need to be prepared with flexible screening and transaction monitoring platforms to respond to any crisis between the west and China over Taiwan.

Businesses with exposure to both Chinese and sanctioning Western jurisdictions need contingency plans in place to respond to the potential deployment of China's own sanctions regime, especially against Western financial institutions.



Andrew Davies

Global Head of Regulatory Affairs,
ComplyAdvantage



Regional and Thematic Review

Europe

[Belarus](#) and its President, Alexander Lukashenko, have provided extensive material support to Russia in its war against Ukraine. In response to this support, as well as Lukashenko's ongoing domestic repression, Western countries have mirrored many Russian designations with similar measures against Belarus. In March and August, the [US](#) targeted a number of state-owned businesses that provide revenue to the regime, officials involved in repression, and – most notably – the Boeing 737 used by the president and his family. In February, the [EU](#) extended previous designations from 2022, and in August, added new measures against individuals and businesses involved in state repression, as well as export bans on firearms, aviation, and space related goods. The UK also designated several Belarusian media organizations, the import of Belarusian gold, goods such as wood, and the export of [UK](#) banknotes and machinery and technology to support the creation of WMD. Belarus's response to Western sanctions has, much like Russia, to try and evade measures and also help Russia in its own efforts. In January, Belarus legalized [digital piracy](#), allowing citizens

to illegally download Western computer programs, film, music, and other media.

In further Russia-linked measures, the US also designated several Russian intelligence operatives in June, including [Konstantin Sapozhnikov](#), who had been involved in organizing protests in **Moldova** in February and March 2023, with a view to organizing a coup in the capital, Chisinau. The US, UK, and EU also expressed concerns about [Russian penetration in Serbia](#), and in July, the US designated [Aleksandar Vulin](#), director of Serbia's security agency, for supporting Russian political interference and criminal activities.

Corruption in the Balkans has also been a major area of focus for the US in 2023, with designations against [corrupt current and former officials](#) in **Bulgaria**, and in **Bosnia**, against the children and companies of Bosnian Serb leader [Milorad Dodik](#). According to the US, the Dodik family have increasingly run the Bosnian Serb region as a private concern for their own enrichment, rather than as a political entity.



Middle East

A major earthquake in **Syria** in February led the [US](#) and [EU](#) to ease its measures against the Assad regime in order to enable deliveries of humanitarian aid to the affected areas. However, Western countries remained focused on the regime's malign activities, and in the spring, the US, UK and EU designated members and associates of the Assad family involved in the production and export of [Captagon](#), a synthetic drug, in collaboration with organized crime and the Lebanese terrorist group, Hezbollah. While the drug has not penetrated most Western markets, it has become popular across the Middle East and especially the Persian Gulf, generating billions of US dollars in revenue for the suppliers. Targeting corruption has also been a theme in the Middle East, with the US, UK, and Canada taking coordinated action against [Riad Salameh](#), the former governor of the central bank of **Lebanon**, and several associates for misappropriating funds and laundering these illicitly into European real estate. As in the European designations, the US and its allies have highlighted the potential role of such corrupt activities in leading to state failure.

Asia-Pacific

Western measures against the [military regime](#) in **Myanmar**, which overthrew the elected government of Win Myint and Aung San Suu Kyi in February 2021, have continued. In a meeting in May, the sanctions authorities of the US, EU, UK, and Canada agreed to [coordinate and align](#) ongoing measures to target those involved in civilian repression. New measures have included designations of businesses providing Myanmar's military with [aviation fuel](#), [state-owned hydrocarbon firms](#) and [financial institutions](#), and officials involved in the [execution of democracy activists](#). In February, the Australian government also announced personal sanctions on [senior Myanmar military figures](#), including the commander-in-chief, Min Aung Hlaing, and his deputy, Soe Win, for their role in the 2021 coup.

Former senior politicians, including former presidents [Mahinda and Gotabaya Rajapaksa](#), officials, and [military officers](#) in **Sri Lanka** were also targeted by the US and Canada for involvement in historic human rights abuses during the Sri Lankan Civil War (1983-2009). During the war, tens of thousands of civilians were killed by the military in their efforts to root out the terrorist group, the [Liberation Tigers of Tamil Eelam \(LTTE\)](#), known as 'The Tamil Tigers.'



Africa

Since 2020, the 'central belt' of African countries has been subject to an [unprecedented number of coups](#) and attempted coups against elected leaders, with successful military takeovers (and even secondary coups) occurring in **Burkina Faso, Guinea, Chad, Sudan, and Mali** from 2020 to 2022. In 2023, this trend continued, with the removal of President [Mohamed Bazoum](#) of **Niger** by his presidential guard in July and President [Ali Bongo](#) of **Gabon** by senior military officers in August. Violence also flared between [rival factions](#) of the military regime in **Sudan** in the spring of 2023, with the paramilitary [Rapid Support Forces \(RSF\)](#) challenging the country's current leader, General [Mohamed Hamdan Dagalo](#).

The [Economic Community of West African States \(ECOWAS\)](#) and the US and former colonial powers with ongoing military, political, and economic commitments in the Sahel and sub-Saharan Africa – France in particular – have expressed grave concerns about these developments. First and foremost, the coups have threatened further instability across the region and have distracted local authorities from the activities of insurgents and terrorists linked to [Islamic State](#). Moreover, they have created power vacuums that others can fill. [France](#) has been asked to withdraw its forces from Mali and Niger by the new military authorities, allowing room for others, such as the Russian paramilitary group [Wagner](#), to offer support in return for commercial opportunities and a blind eye to Russian sanctions evasion schemes. Beyond Mali and Niger, Wagner has been particularly active in the Central African Republic (CAR), Libya and Sudan.

ECOWAS has taken a regional lead in trying to tackle these coups with coercive diplomacy and economic measures, imposing stringent economic sanctions and individual measures on coup leaders in [Mali](#) and [Guinea](#), which in the case of [Mali](#) were loosened in 2022 when the regime promised a democratic transition. This year, ECOWAS imposed tough measures on its fellow member [Niger](#), suspending commercial transactions and freezing state and state-linked assets. While it warned the new military regime in [Gabon](#) of potential intervention, it did not impose sanctions on what was a non-member state.

Over recent years, Western countries have welcomed African leaders taking primary responsibility for tackling regional security challenges, although the US, UK, EU, and others have supported individual designations against individuals involved in creating instability in the region. As a consequence, Western sanctioning authorities have tended to tread carefully in terms of imposing measures that will either undermine tough regional actions (by implying they are Western mandated), or cause further hardship in extremely

poor jurisdictions. Therefore, the primary Western response to the coups of 2023 has been the suspension of US, Canadian, and EU [non-humanitarian aid](#) for Niger and Gabon, rather than harsh restrictive measures – although the EU has created the [legal groundwork](#) for sanctions against Niger if necessary.

The US has taken a much tougher approach towards growing malign Russian influence in Africa. Throughout the year, the US has designated local officials, such as the Malian Defense Minister [Sadio Camara](#) and a range of [Wagner Group](#) representatives and businesses in Mali and the CAR for illicit gold trading, human rights abuses, and sanctions evasion.



Latin America

At the close of 2022, **Haiti** was subject to a range of individual designations from the [US](#), [Canada](#), and the [UK](#) against gang leaders and local politicians who were alleged to have been involved in serious human rights abuses. Further measures were taken in 2023, including the US designation in April of [Gary Bodeau](#), the former president of Haiti's Chamber of Deputies, for corruption and human rights abuse. However, Latin America did provide some positive developments in 2023. Following the agreement of President [Nicolas Maduro's](#) regime in **Venezuela** to talks with the domestic opposition, the US began to ease

sanctions against the country's major export – oil – in early 2023, allowing [limited exports](#) via the US company Chevron, and the development of a [new gas field](#) by Trinidad and Tobago in Venezuelan waters. Progress was confirmed in October, moreover, following the signing of an ['electoral roadmap'](#) between Maduro and the Venezuelan opposition, with the US issuing General Licenses authorizing transactions involving hydrocarbons and gold, and removing the bans on secondary trading in those sectors. If progress continued, the US authorities noted that further relief was possible.



Terrorism

Since the autumn of 2023, global attention has focused on the military conflict between Israel and **Hamas** in the Gaza Strip, following Hamas's terrorist raids into Israel on October 7. A coordinated US-UK response to the attacks has seen [three rounds of sanctions](#) in October and November, targeted on the financial networks supporting Hamas and its allies, the [Palestinian Islamic Jihad \(PIJ\)](#). These have included financial facilitators, money [exchange businesses, and cryptocurrency exchanges](#) in Sudan, Türkiye, Algeria, Qatar, Gaza and Lebanon. The designations have a particular focus on individuals with financial links back to Iran and the IRGC, which analysts believe provides [around 30 percent of Hamas's annual \\$1 billion budget](#).

Although **Hezbollah** has not been actively involved in the conflict between Israel and Hamas it has faced an escalating range of financial sanctions throughout 2023, largely imposed by the US and the UK. As with Hamas, the target of new measures has been the international financial network that supports the group, with new designations of a financial facilitator in [Lebanon](#), the [UK-based art collection](#) of a Hezbollah-linked Lebanese businessman in April, and a [network of Lebanese businessmen and their companies](#) – alleged to be part of Hezbollah's security apparatus – operating across Latin America. The US also alleges that one of those designated, Amer Akil Rada, was involved in the July 1994 bombing of a Jewish cultural center in Buenos Aires.

The US and some of its allies have made a number of other designations against Islamist extremist groups throughout the year, including the joint US-Türkiye targeting of a major **Islamic State** facilitation network led by Islamic State's head of foreign financing, [Brukan al-Khatuni](#), in January 2023. One of the notable aspects of the counter-terrorist developments this year, however, has been the relatively limited nature of coordination between Western states in comparison with actions against Russia or Iran. Both the [EU](#) and [Canada](#) did not make major designations against Hamas-linked individuals or institutions in the wake of the October 7 attack, citing concerns about potential unintended consequences, and the need to focus on resolving the conflict in Gaza first and foremost.



Organized Crime

A further area where the US has continued to apply designations has been organized crime. As noted in several of the designations above – those linked to Syria and Chinese chemical businesses, for example – drugs trafficking remains a significant US concern, with the international traffic in precursors for synthetic opioids, cocaine, and methamphetamines its leading targets. The US has designated members of the Mexican [Sinaloa Cartel](#) involved in sourcing Chinese precursors, [Sinaloa-linked facilitators](#) in the Belgium port of Antwerp, [Jobanis de Jesus Avila Villadiego](#), the leader of the Colombian crime gang the Clan del Golfo, and [Edin Gačanin](#) – known as ‘Europe’s Escobar’, and leader of the Bosnian Tito and Dino Cartel. It has also taken action against the rising violence perpetrated by the Mexican cartels across its southern border, designating senior members of the Cartel de Jalisco Nueva Generacion (CJNG) for [weapons trafficking and Mexican businesses](#) supporting CHANG’s illicit financing operation.

Cybercrime has also been a further focus of Western activity, chiefly by the US, but with occasional support from allies.

In February 2023, the US and UK took joint action - in what was a first for the UK - to designate members of the Russian cybercrime group known as [‘Trickbot’](#) which had targeted Western critical infrastructure during the pandemic. The two countries imposed a further round of sanctions on the group

in [September](#), highlighting the role the group had played in extorting over \$180 million globally from ransomware attacks. In addition, in April, the US also designated the Russia-based website [Genesis Market](#), a major online marketplace for stolen sensitive personal information. The designation coincided with an international [law enforcement operation](#) across 17 countries to permanently take down the site.

2024 Prospects

With such a strong focus on conflicts in Europe and the Middle East, and the ongoing challenges created by Iran and North Korea, it is of little surprise that 2023 has been a year of moderate sanctions activity in other parts of the world. Next year is likely to see ‘more of the same’, although certain trends may well become stronger.

Firstly, the US and several of its allies will continue to target Russian malign influence – often linked to corruption and human rights abuses – in eastern Europe. Indeed, this may well be a stronger area of activity in 2024, as Western countries run out of new Russia-specific targets to designate and seek to ensure that potential loopholes for peripheral sanctions evasion are closed. A similar pattern against Russian proxies, such as Wagner operating in Africa, the Middle East, and possibly Latin America, is also likely to emerge.

Secondly, there is likely to be a renewed focus on terrorist financing of Islamist extremist groups, and especially on state financial support from Iran. Increasingly, Western states are seeing the problem of Islamist terrorism as an issue nurtured by states’ support, and there is likely to be a pronounced move towards trying to tackle terrorist finance ‘at source.’ One uncertain area though remains the level to which US allies in Europe will begin to align with the US approach. So far, there has been reticence, but it seems likely in 2024, pressure on the EU to take new action against Hamas and other Iranian proxies will not be resistible, especially if Israel brings its military action in Gaza to a close.

Thirdly, the US is likely to progressively tighten measures against Mexican cartels involved in the production and supply of opioids into the American market, as well as those threatening civil peace in Mexico itself. In 2024, the instability of Mexico will be a major issue of the US presidential campaign, with Republicans urging tougher action from the Biden administration. Although their rhetoric is unlikely to spark the kinetic measures many want, it will almost certainly lead to

more and tougher designations against the cartels, their allies in the Americas, Europe, and elsewhere – and most problematically – Chinese businesses involved in supplying precursors.

Fourthly, US action against cybercriminals – especially those based in Russia – will continue and intensify. Even though much Russian cybercrime is not state-linked, there is a growing perception that some hostile states are acting as intentional ‘safe havens’ for this kind of crime, and see its deployment against Western countries as a further means of causing pain and disruption. For them, it can be a low-risk/high-reward option. In tackling cybercrime, the US will look more and more to its allies for cooperation – the UK will be a key partner because of its expertise in cyber – and it will look to partners in Europe and Asia-Pacific to support more coordinated takedowns.

Fifthly, Western countries will be mindful of the need to avoid using sanctions to solve every international problem. The moderation of the rate of new designations against non-core targets in recent years suggests that the US and others are aware of the negative consequences of using sanctions in some cases, whether for humanitarian, practical, or reputational reasons. It is notable, for example, how the US, EU, and others have held off from becoming too heavily involved in sanctions against coup leaders in Africa, so far preferring to allow regional players to lead the response. This approach will probably persist in 2024, unless major atrocities and human rights abuses occur. The Biden administration’s slow rapprochement with Venezuela also indicates that – under the president at least – there is a more limited use of sanctions unless there are few other reasonable alternatives.

What does this mean for my firm?

Businesses with exposure to eastern Europe and countries of the former Soviet Union should review screening and transaction monitoring measures to ensure coverage of Russian businesses and politically connected individuals with links to the Putin regime.

Businesses with exposure to sub-Saharan Africa, especially in the metals and mining sector, should screen and monitor client books and transactions for links to potentially suspect Russian proxies.

Businesses with exposure to financial institutions in jurisdictions such as Lebanon, UAE, and Qatar, should review client books and controls for potential links to both Hamas and Hezbollah-linked facilitators, business entities, and charities.

Crypto businesses need to ensure they have appropriate protections and controls in place to detect and monitor for cyber intrusions and cybercrime, whether from state-backed or criminal actors.



Iain Armstrong

Regulatory Affairs Practice Lead,
ComplyAdvantage



Key Sanctions Trends for 2024

In summary, we see six key trends from designating countries which businesses will need to pay attention to in 2024:

01

The decline of UN sanctions, and more autonomous sanctions. Even if US and Chinese relations improve or remain in a 'steady state,' the UNSC will remain blocked as an avenue for shared sanctions action because of Russian recalcitrance. This indicates that more new sanctions are likely to come from regional international organizations such as the EU and ECOWAS, and national governments such as the US, UK, Canada, Japan, and Australia.

02

Greater Western coordination in targeting. Despite the rise of unilateral sanctions, the targets selected will be increasingly coordinated between the US, UK, EU, Canada, and Australia. There will also be increasing incidences of bilateral cooperation on specific issues of mutual concern, such as the US and Türkiye targeting of Islamic state facilitation.

03

Greater focus on effectiveness. Within Western policy communities, a growing body of research focuses on the circumstances in which sanctions appear to work and which they do not. Much of this work points to the need for wide international support and the targeting of the most important economic and financial centers of gravity. This work will increasingly inform and nuance the imposition of sanctions by Western countries in 2024 and beyond.

04

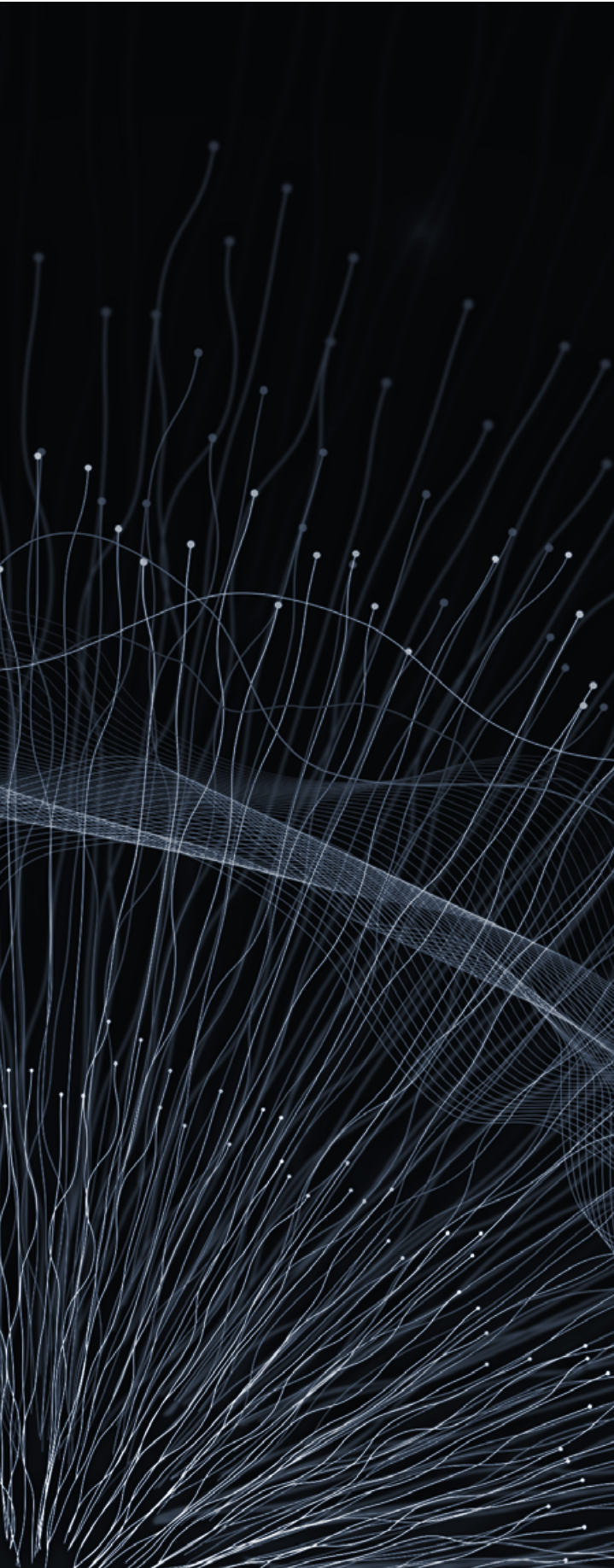
Greater focus on loopholes, workarounds, and evasion. As a result of the focus on effectiveness, governments will look to more quickly identify workarounds and evasion schemes using third countries and alternative payment methods such as cryptocurrency. In 2024, Western countries will seek to close down as many of these loopholes as possible – especially for Russia and Iran – and put increasing pressure on perceived 'weak links,' such as the UAE and Hong Kong (and thus on China), to comply with demonstrable vigor. If they do not, there is likely to be a widening use of secondary measures by the US and a greater willingness by authorities such as the EU to do the same.

05

Increasing international and public-private coordination on implementation. Western countries will also implement more bilateral and multilateral coordinating mechanisms, such as the [partnership](#) between OFAC and the UK's Office of Financial Sanctions Implementation (OFSI) and the REPO Taskforce. There will be increasing impetus for government sector agencies to work more closely with the private sector on active implementation rather than waiting for the private sector to succeed without guidance.

06

Greater focus on unintended consequences. While relying heavily on sanctions, Western countries will likely become more cautious about their potential use in all circumstances. There will be a sustained focus on whether imposing new sanctions can have the desired effect, especially in unstable and poor jurisdictions, and whether such measures will hurt the innocent hardest. There will also be rising action to mitigate unwanted effects within Western countries, especially regarding the risk of over-compliance and [de-banking](#) by financial institutions.



With these trends, businesses must also know how targeted jurisdictions will likely respond to a tighter sanctions net. Based on the past behavior of Iran and North Korea, Russia will resort to more complex evasion schemes for channeling prohibited exports and imports via third-party countries, to which businesses operating in those jurisdictions will need to respond with effective risk management. At this stage, it seems unlikely that a major power such as China will use its own sanctions regime against Western businesses as a countermeasure. Still, there is a potential that a robust Western approach to sanctioning Chinese businesses linked to Russian and Iranian evasion, or the supply of opioid precursors to the Americas, might stimulate tougher measures against Western financial institutions and technology firms operating in Asia-Pacific.

What does this mean for my firm?

In our State of Financial Crime survey,

41%

of firms said a limited ability to screen against sanctions and watchlists was a main limitation in the approach to financial crime detection.

This has to change in 2024. Compliance teams must have screening systems with real-time updates to rapidly changing lists.

They should also ensure their transaction monitoring systems are easily configurable to identify risks. PEP and adverse media screening must be effectively deployed to tackle 'unknown unknown' sanctions risk. Finally, compliance leaders should ensure they are proactively working with the best risk data so the business is taking a forward-leaning approach that regulators will welcome.



Alia Mahmud

Global Regulatory Affairs Practice
Lead, ComplyAdvantage

- [↑](#) Back to beginning
- [←](#) Previous section
- [→](#) Next section

Regional Regulatory Trends




Global AML/CFT Developments

The world will continue to look to the FATF to identify risks, update standards, and issue guidance to improve the fight against money laundering, terrorist financing, and proliferation financing. It is essential for financial crime teams to stay abreast of developments at the FATF level, as new guidance and standards are generally adopted as national law, which can aid firms in identifying and managing emerging financial crime risks.

Indonesia was recently announced as a new member, and Russia's membership remains suspended. Bulgaria was recently added to the FATF's grey list, and Albania was removed alongside the Cayman Islands, Jordan, and Panama. The following 23 countries, including international finance hub the UAE, EU members Bulgaria and Croatia, and other large markets such as Nigeria and South Africa, remain on the grey list:

FATF Grey List – November 2023



- Barbados
- Bulgaria
- Burkina Faso
- Cameroon
- Democratic Republic of Congo
- Croatia
- Gibraltar
- Haiti
- Jamaica
- Mali
- Mozambique
- Nigeria
- Philippines
- Senegal
- South Africa
- South Sudan
- Syria
- Tanzania
- Türkiye
- Uganda
- United Arab Emirates
- Vietnam
- Yemen

High-risk countries on the black list remain the DPRK, Iran, and Myanmar. The FATF will also hold 29 mutual evaluations through 2024, which could result in a swathe of new local AML/CFT laws and regulations, including India, Jersey, Guernsey, Iraq, BVI, El Salvador, Argentina, and Oman. A complete list of mutual evaluations is included in Appendix B. The FATF Plenary will select a new president to start a two-year term in [July 2024](#), when the Singaporean Presidency held by Raja T. Kumar ends. Until that point, work will continue under the 2022-2024 priorities, which include:

- Strengthening asset recovery;
- Countering illicit finance of cyber-enabled crime;
- Increasing the effectiveness of global AML/CFT measures;
- and reinforcing partnerships with FATF-Style Regional Bodies (FSRBs).

During the October plenary, the FATF agreed to revise its standards further and publish several papers.

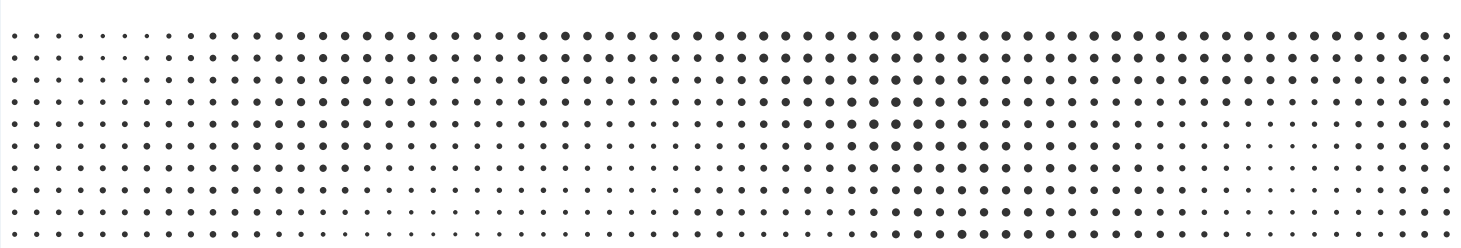
The updated [standards](#) include changes to the following Recommendations related to asset recovery and associated Interpretative Notes to the Recommendations (INR): R4 to R30, R31, R38, and R40. Changes include requiring countries to prioritize asset recovery, introduce non-conviction-based confiscation, implement extended confiscation to deprive criminals of their lifestyles, introduce powers to suspend or withhold consent to transactions, promote expedited asset freezes and seizures, and recognize another country's preliminary and final court orders. This will likely impact firms' SAR regimes. The FATF also recently published a report focusing on Asset Recovery [Inter-Agency Networks](#) (ARINs), which includes a review of ARINs, their impact, and the challenges they face, which may be relevant for firms involved in public-private partnerships or regularly dealing with law enforcement. The FATF also updated R8 and its INR to limit unintended consequences on [non-profit organizations](#)

(NPOs). It calls on countries to identify NPOs that fall within the scope of the FATF definition. It also published an updated paper on [best practices](#) to fight terrorist financing abuse of NPOs without affecting legitimate activities, which includes a section for financial institutions. The FATF issued a report focusing on [crowdfunding](#) for TF, illicit finance from [cyber-enabled fraud](#), and the misuse of citizenship and residency by [investment programs](#). The FATF will also release public guidance at its February 2024 Plenary on R25, which covers beneficial ownership and the transparency of legal arrangements.

The International Monetary Fund (IMF), whose work often complements that of the FATF, reviewed its [AML/CFT Strategy](#) covering elements of its financial integrity work. It is anticipated that this will inform the work of the IMF into 2024. In a recent report on the cross-border money laundering risks in the [Nordic-Baltic](#) region, the IMF took a different approach to the FATF evaluations and included an analysis of financial flow data and payment data, the size of financial centers in-country, and other macroeconomic markers and risks, such as the threat to financial stability posed by money laundering and impact on funding and liquidity. The IMF also used machine learning to analyze financial integrity surveillance data. [Civil society organizations](#) welcomed this approach as a way to complement the FATF's mutual evaluation process.

The Wolfsberg Group will continue to publish best practice standards and guidance into 2024 for financial institutions. In 2023, it issued numerous publications, including the following:

- Central Bank [Due Diligence Questionnaire \(CBDDQ\)](#), [Financial Crime Compliance Questionnaire \(FCCQ\)](#), Guidance, Glossary and FAQs
- [ABC Guidance](#)
- [Request for Information \(RFI\)](#) Best Practice Guidance in Simplified Chinese
- Updated [Payment Transparency](#) Standards



Crypto Asset Digital Framework

Global standard setters and international organizations, including the Financial Stability Board (FSB), the FATF, the IMF, and IOSCO, will continue to develop policy recommendations and standards in the crypto asset space to build a digital framework to manage risks for adoption by different countries. In October 2023, the [G20](#) adopted a Roadmap on Crypto Assets. This followed calls by G20 leaders at the Delhi Summit to regulate and supervise crypto assets effectively to manage money laundering and proliferation financing risks. The Policy Implementation Roadmap is included in the IMF-FSB [Synthesis Paper](#), which sets out policies for crypto assets. This paper was developed following the FSB report for [regulating and supervising crypto-asset activities and markets](#) which includes ten key recommendations for countries to consider when looking to regulate crypto, including regulatory powers and tools,

cross-border cooperation, coordination, and information sharing, governance, risk management including appropriate AML/CFT standards, data collection recording, and reporting, disclosures, addressing financial stability risks arising from interconnections and interdependencies, and comprehensive regulation of crypto asset service providers with multiple functions. The Synthesis Paper builds on that report and discusses the implications of crypto-assets, including macroeconomic stability, financial stability, regulatory issues, and other risks. It further includes an overview of policy and regulatory responses to identified risks. The G20 Roadmap, which should be implemented by the end of 2025, focuses on four critical overarching actions with a sub-set of actions, lists the organizations responsible for carrying these out, and has an accompanying timeline. The four main actions are:



01. The implementation of policy frameworks.
02. Outreach beyond G20 jurisdictions.
03. Global coordination,
04. Addressing data gaps.



Regarding AML/CFT and financial integrity risks, countries are called on in the IMF-FSB report to implement FATF standards. At the [FATF Plenary](#) in February, the FATF agreed on a roadmap to speed up global adoption of AML/CFT measures, supervise crypto assets, and take steps to supervise crypto assets in the first half of 2024. In June, the FATF published a [Targeted Update](#) on the Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. When assessing progress on R.15, which requires countries to apply AML/CFT measures to VASPs, the FATF found that only one jurisdiction is fully compliant. 24 jurisdictions are largely compliant, 50 are partially compliant, and 23 are not compliant. Key challenges remain around carrying out a risk assessment, building a registration or licensing regime for VASPs, and implementing the Travel Rule. The FATF found insufficient progress has been made on Travel Rule implementation, with only 35 jurisdictions passing laws or regulations and 27 countries in the process of building laws and regulations. The report further identified emerging risks. This includes the use of virtual assets for proliferation and terrorist financing, with DPRK having stolen \$1.2 billion since 2017 and increases in the use of virtual assets for terrorist financing to ISIL, Al Qaeda, and affiliates. In the Decentralized Finance (DeFi) space, \$1.1 billion was stolen in 2022. Additional emerging risks were identified as misusing unhosted wallets, non-fungible tokens (NFTs), and stablecoins.

The FSB also issued a report providing high-level recommendations on regulating global stablecoin (GSC) arrangements in July 2023. The report comprises a set of ten recommendations for national authorities to address financial stability risks and is meant to complement other international guidance. Of note to financial crime professionals are recommendations on the need to have comprehensive governance and risk management frameworks, [“especially with regard to operational resilience, cyber security safeguards and AML/CFT measures, as well as “fit and proper” requirements,”](#) and that GSC comply with all regulatory and supervisory requirements before operating in a particular country.

The International Organization of Securities Commission (IOSCO) issued its [Final Report](#) with Policy Recommendations for Crypto and Digital Asset Markets to ensure crypto assets “meet the standards of business conduct that apply in [traditional financial markets.”](#) The IOSCO report covers the following topics and includes standards, recommendations, and examples of good practice: conflict of interests, market manipulation, insider trading and fraud, custody, client asset protection, cross-border risks and regulatory cooperation, operational and technological risk, and retail distribution. The report includes recommendations and measures relevant to financial crime and money laundering, such as the need for international cooperation, developing a globally consistent and coordinated approach to regulating crypto, and the importance of enforcement action.

The United States

In the US, as firms figure out how to comply with the Corporate Transparency Act (CTA), the government will continue to explore legislation and regulation to manage the risks of technological innovation, with AML/CFT remaining a national security concern. It remains to be seen whether the Establishing New Authorities for Businesses Laundering and Enabling Risks to Security (ENABLERS) Act, extending AML/CFT requirements to professional service providers such as accountants, lawyers, and third-party payment services, will make a comeback after the [Senate blocked its inclusion](#) in the NDAA 2022.

FinCEN Priorities & The Corporate Transparency Act

FinCEN will continue to lead the US's fight against illicit finance into 2024 under new leadership. In July 2023, Andrea Gacki, who previously served as Director of OFAC, was appointed the new Director of FinCEN. During 2023, FinCEN officials met with counterparts in [South Africa](#) to discuss illegal wildlife trafficking and human smuggling, and in [Mexico](#) to discuss fentanyl trafficking. It issued alerts on COVID-19 employee retention [credit fraud](#), [terrorist financing by Hamas](#), [pig butchering](#), Russian [export control evasion](#), [mail-theft](#)-related check fraud schemes, and [human smuggling](#). FinCEN also held public-private roundtables on Russia's attempts to [evade sanctions export controls](#), [cyber-related terrorism financing](#), and [DPRK's illicit cyber activities](#).

The [CTA](#) introduces requirements around beneficial ownership transparency in the US and comes into force on January 1, 2024. In 2020, the US passed the National Defense Authorization Act 2021 (NDAA) and Anti-Money Laundering Act (AMLA), which included the CTA banning anonymous shell companies and requiring firms to report their beneficial owners to the government. It developed a new category of entities required to comply with the law as ["reporting companies"](#) and set out requirements for these companies to keep a record of their shareholders or ultimate beneficial owners (UBOs) and report this information and any subsequent updates to FinCEN. [A beneficial owner](#) is an individual who owns or controls (directly or indirectly) at least 25 percent of the ownership interest or exercises substantial control over an entity. Beneficial ownership information includes (BOI): full name, date of birth,

current address, and a distinctive identification number. In November 2023, FinCEN issued a rule detailing how to use an [entity FinCEN identifier](#) to report BOI if three conditions are met:

01

The entity has obtained a FinCEN identifier and provided that FinCEN identifier to the reporting company.

02

An individual is or may be a beneficial owner of the reporting company by virtue of an interest in the reporting company that the individual holds through the entity.

03

The beneficial owners of the entity and the reporting company are the same individuals.

An entity FinCEN identifier is a unique identifying number issued to reporting companies that have filed their initial BOI reports with FinCEN. The CTA applies to US entities and foreign entities doing business in the US. New reporting requirements come into effect on January 1, 2024, with companies that are already incorporated required to share BOI by January 1, 2025, and companies established after 1 January 2024 required to share BOI with FinCEN within 30 days. In September 2023, however, FinCEN proposed to [extend the filing deadline](#) for businesses created during the first year requirements apply (between January 1, 2024, and January 1, 2025) from 30 days to 90 to allow additional time to understand the requirements. After January 1, 2025, the filing deadline will remain 30 days from incorporation. Company directors that do not comply could pay up to \$500 per day (up to \$10,000) and face jail time of up to 2 years. Businesses will need to update FinCEN with any material changes. FinCEN published a notice of proposed rulemaking in December 2022 detailing who may have [access to BOI](#) contained in the FinCEN database. This includes domestic government agencies (including federal agencies working in national security, intelligence and law enforcement, Treasury officers, and state, local, and tribal law enforcement agencies), authorized foreign requesters such as foreign law enforcement agencies, judges, prosecutors, central authorities, or competent authorities

via federal intermediary agencies, and financial institutions and regulatory agencies to meet CDD compliance requirements. Financial institutions must have a company's consent to access that information and have in place certain administrative, technical, and physical safeguards to protect the confidentiality of BOI, including security standards. There are no further details on how financial institutions will access BOI information. FinCEN has issued [Beneficial Ownership Information Reporting Guidance](#), including FAQs, key filing dates and questions, and a [Small Entity Beneficial Ownership Information \(BOI\)](#) guide to help companies comply with the CTA. FinCEN will publish additional guidance and educational materials [here](#), including videos, infographics, and compliance guides. In the proposed rulemaking on [access to BOI](#), it was noted that FinCEN continues "to face resource constraints in developing and deploying the Beneficial Ownership IT System" but

anticipates a go-live date of January 1, 2024. FinCEN has requested an additional \$38.7 million for the [2024 budget](#) to support implementation of CTA and AMLA.

Crypto and AI

With regards to addressing emerging threats related to technological innovation, there are two critical areas of focus that will occupy US regulators in 2024: crypto assets and artificial intelligence (AI).

In the crypto space, 2024 may see numerous pieces of legislation passed following the flurry of legislative proposals put forward in 2023 in response to the collapse of FTX. In July 2023, [seven separate bills](#) were put forward in Congress to regulate crypto:

Bill number	Bill title	Sponsor	Date	Vote Results
HR 4763	Financial Innovation and Technology for the 21st Century Act (Financial Services Committee)	Rep. French Hill	July 26	House Financial Services: 35 - 15
HR 1747	Blockchain Regulatory Certainty Act	Rep. Tom Emmer	July 26	House Financial Services: 29 - 21
HR 2969	Financial Technology and Protection Act of 2023	Rep. Zach Nunn/ Rep. Jim Himes	July 26	House Financial Services: 50 - 0
S 2226	National Defense Authorization Act for Fiscal Year 2024 (S.A. 1087 Manager's Amendment)	Sen. Jack Reed	July 27	On July 27, a Senate vote passed the Managers Amendment to the NDAA by 94 - 3 that included Bank Secrecy Act provision for crypto.
HR 4763	Financial Innovation and Technology for the 21st Century Act (House Agriculture Committee)	Rep G.T. Thompson	July 27	House Agriculture Committee: Voice Vote
HR 4766	Clarity for Payment Stablecoins Act of 2023	Rep. Patrick McHenry	July 27	House Financial Services 34 - 16
HR 4841	Keep Your Coins Act of 2023	Rep. Warren Davidson	July 27	House Financial Services 29 - 21

Source: Forbes

Key additional pieces of legislation in AML/CFT include the Crypto-Asset National Security Enhancement and Enforcement ([CANSEE](#)) Act and the [Digital Asset Anti-Money Laundering Act of 2023](#). CANSEE looks “to prevent money laundering and stop crypto-facilitated crime and sanctions violations” and would bring DeFi services into the scope of AML/CFT legislation. The Digital Asset AML Act was proposed to mitigate the risks to national security by extending BSA/AML responsibilities to “digital asset wallet providers, miners, validators, and other network participants that may act to validate, secure, or facilitate digital asset transactions.” It would also address risks of unhosted wallets by requiring banks and MSBs to verify customer and counterparty identities and file reports on transactions involving unhosted wallets or wallets in non-BSA-compliant jurisdictions. It would call on FinCEN to issue guidance for financial institutions on the risks of digital assets linked to anonymity-enhancing technologies, extend BSA foreign bank account reporting rules to include digital assets, and require digital asset ATM owners to regularly submit and update the physical address of the ATMs owned or operated and verify the identity of customers and counterparties. In October 2023, FinCEN issued a notice of [proposed rulemaking](#) designating [convertible virtual currency mixing \(CVC mixing\)](#) as a type of transaction of primary concern regarding money laundering. The objective is to enhance the transparency of CVC mixing to fight terrorist financing and proliferation financing, given links between CVC mixing to Hamas, Palestinian Islamic Jihad, and North Korea.

The US will likely play a leadership role on the international stage in the development of global AI standards. The US does not yet have national legislation, but the White House has issued several executive orders and has called on Congress to develop data privacy legislation. Numerous states have also introduced AI legislation. [An Executive Order](#) on Safe, Secure, and Trustworthy Artificial Intelligence issued in October 2023 calls for the measures to support the following actions:

- New standards for AI safety and security, including sharing safety test results with the US government and protecting Americans from AI-enabled fraud and deception, amongst other measures.
- Protecting Americans’ privacy, including by calling on Congress to pass data privacy legislation and to explore the use of privacy-preserving solutions.

- Advancing equity and civil rights, building on the [Blueprint for an AI Bill of Rights](#) and the [Executive Order directing agencies to combat algorithmic discrimination](#), address algorithmic discrimination and bias, and develop best practices for fairness in criminal justice.
- Promoting innovation and competition, supporting measures to catalyze AI research.
- Advancing American leadership abroad by working with other countries and speeding up the development and adoption of AI standards.
- Ensuring responsible and effective government use of AI by issuing appropriate guidance and hiring AI professionals.



Various states have [proposed AI legislation](#) that could impact the use of AI in AML/CFT programs. The laws cover topics such as consumer protection, user data, security, the use of bots, bias, and automated decision systems (ADS). They could have implications for the use of facial recognition as part of onboarding and automated decision-making and profiling around risk assessments, triaging of alerts and matches during adverse press and sanctions screening, and transaction monitoring solutions using AI. States that have enacted legislation that affects the use of AI relevant to financial crime professionals include California, Connecticut, Colorado, Illinois, Indiana, Maryland, Montana, New York, Tennessee, and Texas. States that have proposed additional legislation relevant to AI include California, Connecticut, the District of Columbia, Maine, Massachusetts, New Hampshire, New Jersey, Oregon, Pennsylvania, Rhode Island, South Carolina, Vermont, and Virginia. Further details of additional state-level AI laws are available [here](#).

SEC Priorities

The US Securities and Exchange Commission (SEC) published its [2024 Examination Priorities](#) citing the following risk areas that impact market participants: information security and operational resilience, crypto assets and emerging financial technology, regulation systems compliance and integrity, and anti-money laundering. The SEC will examine investment advisors, investment companies, broker-dealers, clearing agencies, and categories of self-regulatory organizations.





Canada


Canada will continue to modernize and strengthen its AML/CFT regime through 2024 by implementing the measures it unveiled in the 2023 budget. The country currently holds the Vice Presidency of the FATF, which began in July 2023. A key change is establishing the Canada Financial Crimes Agency (CFCA) to respond to complex cases of financial crime. The CFCA “will become Canada’s lead enforcement agency against financial crime” and bring together experts to increase prosecutions, convictions, and asset forfeitures, as well as money laundering charges in Canada. Public Safety Canada has been given \$2 million to design the CFCA, its structure, and its mandate.

The government will also introduce numerous amendments to Canadian legislation in 2024. Amendments to the Criminal Code and the Proceeds of Crime (Money Laundering and Terrorist Financing Act) (PCMLTFA) will strengthen tools to make investigation, enforcement, and information sharing more effective. Specific measures include:

- Give law enforcement the ability to freeze and seize virtual assets.
- Improve financial intelligence information sharing between national authorities.
- Introduce an offense of structuring financial transactions to avoid reporting obligations to FINTRAC.
- Carry out criminal record checks and strengthen registration of currency dealers and MSBs.
- Criminalize operating an unregistered MSB.
- Give FINTRAC powers to share strategic intelligence related to the financing of threats to the safety of citizens.
- Protect whistleblowers reporting to FINTRAC.
- Allow for the use of non-compliance reports by FINTRAC in criminal investigations.
- Require financial institutions to report sanctions-related information to FINTRAC.

Canada will continue to build its national publicly accessible federal beneficial ownership registry. Under the Canada Business Corporations Act, the national beneficial ownership register will allow access to beneficial ownership data held by participating provinces and territories. Canada is also reassessing its supervisory framework by expanding the mandate of the Office of the Superintendent of Financial Institutions (OSFI) to federally regulated financial institutions (FRFIs) and receiving FINTRAC disclosures. Supervision will include assessing whether FRFIs have adequate policies and procedures in place to protect their security and integrity against foreign interference. National authorities will also be given powers to take control of an FRFI, issue a direction of compliance, and allow the finance minister to impose enhanced due diligence requirements. These proposed changes will result in amendments to the Bank Act, the Insurance Companies Act, the Trust and Loan Companies Act, and the Office of the Superintendent of Financial Institutions Act, in addition to the PCMLTFA. Lastly, to protect Canadians from risks associated with crypto-assets following the failure of FTX and Signature Bank, OSFI will issue guidelines for financial institutions to disclose exposure to crypto-assets, and the government will introduce the requirement for federally regulated pension funds to disclose crypto-asset exposures to OSFI.

The [2023 Fall Economic Statement](#) announced additional proposed changes to the PCMLTFA. This includes extending PCMLTFS requirements to intermediary companies or "acquirers" offering cash withdrawal services to title insurers. It will also require real estate representatives to identify third parties and unrepresented parties in real estate transactions to tackle fraud and money laundering in real estate. It will combat sanctions evasion and environmental crime by allowing FINTRAC to develop intelligence products and disclose findings to support law enforcement action. The government will also propose changes to the Criminal Code by amending the money laundering offenses to prosecute third-party money launderers better and adapt production orders and financial data. The government will also create a Trade Transparency Unit within the Canada Border Service Agency to address trade-based financial crime. In 2020, it was estimated that \$45 - \$113 billion is laundered each year in Canada.

An aerial, high-angle photograph of a city skyline, featuring the CN Tower as the central focal point. The image is in grayscale, with a dark, moody atmosphere. The buildings are densely packed, and the water of a harbor or bay is visible in the background. The overall composition is vertical, matching the page layout.

**Canada will
continue to
build its
national publicly
accessible
federal beneficial
ownership
registry.**

The EU, France, and Germany

EU AML Package

It is anticipated that the EU's latest AML package will be agreed in Q1 2024, followed by a three-year transition period. It was introduced following a series of AML/CFT scandals that rocked members of the European Union and to harmonize AML/CFT measures across the EU. The package consists of four separate instruments: (1) A regulation to establish an AML Authority (AMLA), which is anticipated in 2024; (2) A new 6th Anti-Money Laundering Directive for countries to improve their domestic AML/CFT frameworks; (3) A new piece of regulation providing more clarity and guidance for obliged entities required to meet AML/CFT obligations, and (4) An updated Transfer of Funds Regulations (TFRs) clarifying requirements for information accompanying crypto asset transfers. The TFRs were adopted in June 2023.

The regulations around AMLA would create an integrated AML/CFT supervisory system promoting cooperation and implementation of harmonized rules with the AMLA at its center. AMLA will have direct supervision over the "riskiest" 40 obliged entities for a period of three years. It will be able to obtain documents and information, carry out on-site visits, and impose financial sanctions. It is anticipated that AMLA will employ 250 staff members. A call for applications to host AMLA was launched alongside selection criteria for the AML headquarters. The location should allow AMLA to execute its duties and powers fully, facilitate the recruitment of qualified and specialized persons, provide appropriate training opportunities, and allow for close cooperation with other parts of the EU. Additional criteria include that the host jurisdiction must adequately manage the risks of money laundering and terrorist financing.

The 6th AMLD repeals previous MLDs, introduces changes to align practices between national authorities and FIUs across Europe, and ensures convergence and cooperation between national authorities. It clarifies the

powers of FIUs and provides feedback to obliged entities on SARs. It also requires countries to conduct a national risk assessment every four years. It details the powers and tasks of supervisors, introduces a duty of oversight on self-regulatory bodies, and promotes risk-based supervision. It also expands upon beneficial ownership registrars' powers to maintain accurate, adequate, and up-to-date information. Access to BO registers will be granted to journalists and civil society organizations deemed to have a legitimate interest. Rights of access will be valid for two and a half years. 6AMLD also clarifies the legal basis of processing personal data to prevent money laundering and terrorist financing. It will also require the establishment of a central register detailing information on AML/CFT shared by obliged entities.

The new regulations on AML/CFT for obliged entities look to apply AML/CFT requirements consistently across the EU. The regulations broaden the definition of obliged entities to cover persons providing certain cryptoasset activities, unlicensed crowdfunding platforms, football clubs/agents, and persons involved in luxury commerce. They will be required to have AML/CFT controls in place. It further details how firms should organize their internal AML/CFT systems and controls, provides evidence that they understand risks and have adequate risk assessments in place, and includes provisions on due diligence. It outlines more detailed requirements on UBOs, including thresholds and how to determine control, and additional details on other aspects of AML/CFT programs, including managing higher-risk situations, such as PEPs, ongoing monitoring, reliance and outsourcing, training and awareness, submission of SARs and record-keeping. It further contains provisions for "golden passports" and visas and caps for cash payments for individuals providing goods and services. AMLA will be issuing technical standards, which firms operating in Europe should review to ensure compliance with new measures.



The EU has proposed changes to an [AI Act](#) which looks to harmonize the regulation of AI across Europe, which it hoped to finalize in 2023. It also published a list of “Prominent Public Functions” with a list of titles which should, in theory, make it easier to determine whether or not somebody is a PEP. The European Commission updated its list of [high-risk third countries](#), adding the following countries to the existing list: Cameroon, the Democratic Republic of the Congo, Gibraltar, Mozambique, Nigeria, South Africa, Tanzania, Vietnam, and, controversially, the UAE.

Finally, The EBA and the European Data Protection Board (EDPB) will be issuing guidance on data protection and crypto. The EBA's [2024 work program](#) highlighted that it would prepare for the transition to the new AML/CFT framework. The European Commission also proposed a [Payment Services Directive 3](#), which included measures to tackle payment fraud, new rules for the authorization of non-bank payment service providers (PSPs), and other data protection provisions.

MiCA & TFR

The Markets in Crypto-Assets (MiCA) and Transfer of Funds Regulations (TFR) issued in June 2023 created a new foundation for how crypto-assets will be regulated in the EU. MiCA regulates crypto-assets not covered by existing legislation, such as MiFID II. ESMA will issue guidance by December 30, 2023, to distinguish which crypto-assets fall under MiCA and which fall under MiFID II. The following are classed as regulated services:

- Providing custody and administration of crypto-assets on behalf of clients.
- Operating a trading platform for crypto-assets.
- Exchanging crypto-assets for funds or other crypto-assets.
- Executing orders for crypto-assets on behalf of clients.
- Providing advice on crypto-assets.

MiCA does not apply to non-fungible tokens. It also imposes requirements such as having persons that are fit and proper in senior management, having in place adequate controls and risk management systems, and adequate processes and procedures to preserve market integrity and confidentiality. While requirements for asset-referenced tokens in Title III and e-money issuers in Title IV are applicable from June 2024, other requirements in MiCA apply from December 30, 2024.

The updated TFRs, which were part of the AML package, introduce requirements for specific information to accompany crypto-asset transfers and how the information should be submitted. This includes:

- Name of originator.
- The distributed ledger address or crypto-asset account number of the originator.
- The address (including the country) of the originator.
- A personal document number and customer identification number – where that is not available, the originator's date of birth, place of birth of the originator.
- Legal Entity Identifier – where that is not available, another official identifier of an originator legal entity.
- Name of beneficiary.
- The distributed ledger address or crypto-asset account number of the beneficiary.
- The address (including the country) of the beneficiary.
- A personal document number and customer identification number – where that is not available, the originator's date of birth, place of birth of the beneficiary.
- Legal Entity Identifier – where that is not available, another official identifier of a beneficiary legal entity.

Originator and beneficiary information should be submitted before or at the same time as the transfer is made and should be subject to stringent security controls. Firms should also have policies and procedures in place to monitor for missing information. The law covers transfers higher than €1,000 from self-hosted wallets. The TFR applies from December 30, 2024.

The EBA released [draft travel rule guidelines](#) in November 2023 for consultation until February 26, 2024. It covers required accompanying information for transfers to or from self-hosted wallets, how to transmit such information using a secure system, the need to have processes for identifying, documenting, and dealing with transfers and document transfers with missing and incomplete information. The guidelines will become effective from December 30, 2024.



France

French authorities will expect firms to comply with new provisions and changes to regulations introduced in 2023. In March, the French Ministry of the Economy issued a [decree](#) changing the definition of PEPs and expanding the scope of AML/CFT regulations. It established a list of national politically exposed functions to align with EU AML/CFT directives, including political, judicial, and other relevant high-level political functions and state-owned enterprises. An additional [decree](#) was issued in February 2023 on customer identity verification for low-risk products and services.

The AMF [amended](#) its general [regulation](#) and doctrine regulating Digital Assets Service Providers (DASPs) to align with MiCA, which is effective from January 1, 2024. The changes were introduced to integrate enhanced provisions for registration introduced by the DDADUE law and to match the requirements of DASP authorization to those set out under MiCA. This includes having adequate security and internal controls, resilient and secure IT systems, monitoring conflicts of interest, providing clear, accurate, and non-misleading information, having specific custody provisions, prohibiting the use of customer assets without consent, and having signed agreements with customers. The updated regulation and the following updated documents on DASPs also come into force on January 1, 2024:

- DOC-2019-23 (preparation of a registration and authorization dossier)
- DOC-2019-24 (repository of cybersecurity requirements)
- Position-Recommendation DOC-2020-07 (Questions and answers on the DASP scheme)

DASPs whose registrations were approved before this date must comply with new provisions as of January 1, 2024. It is no longer possible to submit a simple registration application to become a DASP. A strengthened registration application or an optional authorization must be submitted.

TRACFIN published an updated [AML/CFT: Threat Status](#) report which includes an overview of vehicles used to launder funds and finance terrorism, sectors exposed to ML/TF, and the types of predicate offenses associated with this alongside case studies, typologies that could be used to support ongoing monitoring of customers and clients. Firms should review this document to identify examples that could be used for staff training and development but also to identify risk indicators for ML/TF.

Germany

Germany will continue to implement provisions set out under the draft "Improving the Fight Against Financial Crime" (KKBG) bill [passed in October](#), which addresses deficiencies identified under the FATF 2022 Mutual Evaluation. The KKBG has been passed to restructure and re-envisage powers to fight financial crime in Germany, improving the methods and tools employed. This includes setting up a new AML "super-agency" – the Federal Office for Fighting Financial Crime (BBF) – establishing a new money laundering investigations hub to more effectively prosecute money laundering cases, transferring the Central Office for Financial Transaction Investigations (FIU) and the Central Office for Sanctions Enforcement (ZfS) into the BBF by mid-2025. It will also allow for the establishment of a Central Office for Money Laundering Oversight, which will issue uniform guidelines to ensure a coordinated approach to by supervisory authorities across the non-financial sector. The BBF will have a register of real estate transactions, allowing authorities access to fight money laundering and enforce sanctions. Additional reforms include the ability to carry out administrative asset investigations and identify "economic beneficiaries" of suspected proceeds of crime.

Numerous other [amendments](#) were introduced. For example, financial holding companies, mixed financial holding companies, and insurance holding companies should comply with the Anti-Money Laundering Act. Obligated entities not registered with GoAML, the FIUs reporting portal, will be subject to a fine by January 1, 2024, with new fines issued for non-compliance as of January 1, 2027. With regards to corporate transparency, beneficial ownership information detailing "place of birth" will be required as of January 1, 2027. Associations and legal structures required to comply with transparency register obligations should provide transfer overviews of ownership and control structures by July 1, 2025, and authorized persons must be introduced for reports to the register by January 1, 2025.

Additional changes apply to obliged entities. These include the need to file a criminal charge or a demand for prosecution to the FIU, notify the FIU when a SAR is filed, and obtain consent to process transactions from the FIU only (no longer the public prosecutors' office). The bill also introduces a "tipping off" offence-like prohibition of making others aware of investigative measures carried out by the Central Sanctions Enforcement Office.



Other European Countries

Additional regulatory changes and guidance issued by European countries that may impact firms into 2024 include:

- Bulgaria and Croatia have been added to the FATF grey list and will likely update national laws and regulations to improve their AML/CFT frameworks.
- Ireland adopted [European Union \(Anti-Money Laundering: Beneficial Ownership of Corporate Entities\) \(Amendment\) Regulations](#) aligning the definition of “high-risk third country” to the EU and detailing access to Ireland’s central registers solely where there is ‘legitimate interest.’
- Italy’s FIU published provisions on [AML anomaly detection](#), [IVASS](#) launched a consultation on AML/CFT measures by firms, and the Bank of Italy published guidance on AML requirements for [private banking](#).
- Latvia has put forward a bill amending the [Anti Money Laundering and Counter-Terrorism and Proliferation Financing \(AML/CTPF\) Act](#) alongside amendments to the [Enterprise Registry Act](#). Changes include amending the definition of UBOs as they apply to trusts, requiring trustees to retain and update UBO information and disclose such information under certain circumstances, making UBO information available the day after amendments to the AML/CTPF Act have taken place, and requiring CDD to be carried out on transactions above €500. Changes are expected to be implemented by [January 6, 2025](#).
- In the Netherlands, the Ministry of Finance carried out a [consultation](#) on the Markets in Crypto Asset Regulation Implementation Act, a consultation on a Regulation on Information to Accompany [Transfers of Funds and Transfers of Crypto Assets](#) and a consultation on proposed amendments limiting [access to UBO registers](#). The Dutch Banking Association issued new NVB standards [for risk-based money laundering investigations](#).
- [Spain](#) launched a Central Register of Beneficial Owners under Royal Decree 609/2023 that will be available initially to national authorities and then to Spanish-obliged persons. However, firms cannot solely rely on the register and must carry out additional checks.
- Sweden has amended the Money Laundering Act to increase penalties for AML/CFT breaches by [gambling operators](#) that would come into effect on April 1, 2024.
- [Switzerland](#) will present new AML/CFT rules to Parliament in 2024 bringing into scope lawyers and consultants who work in real estate or set up legal entities and arrangements. They will also introduce tighter requirements for regulated firms to manage sanctions evasion. The country also plans to create a beneficial ownership registry at the Federal Department of Justice and Police. FINMA recently published a [guidance](#) on money laundering risk analysis.

The United Kingdom

2023 was a watershed moment in the UK's fight against illicit finance, with the government enacting the hefty Economic Crime and Corporate Transparency Act (ECCTA) 2023 and publishing the Economic Crime Plan. The ECCTA introduced numerous reforms to make the UK hostile to illicit financial flows. It created a new [failure to prevent fraud](#) offense that applies to firms with more than 250 employees, £36 million turnover, and £18 million in total assets. It also granted new [powers](#) to the Companies House Registrar that will allow it to clean up Companies House, request additional information related to Companies House filings, take action where information is not forthcoming, and proactively share data in certain circumstances. Additional Companies House reforms require identity verification for all company directors and 'People with Significant Control,' whether directly with Companies House or via a new type of service provider – [Authorised Corporate Service Providers \(ACSPs\)](#), who must register with a supervisory body to comply with AML requirements. ECCTA also introduced provisions to improve beneficial ownership transparency, including providing and retaining more useful information and limiting the abuse of limited partnerships. Regarding [crypto assets](#), ECCTA includes changes to the Proceeds of Crime Act 2002, introducing powers to seize and recover crypto assets. ECCTA also introduces information-sharing provisions to allow regulated financial institutions subject to AML regulations to [share information](#) directly or via a third-party intermediary for businesses in the financial sector and includes appropriate safeguards to ensure consumer access to products. ECCTA further enhanced intelligence-gathering powers for law enforcement.

The UK published an [Economic Crime Plan 2 \(ECP2\)](#) and a [National Fraud Strategy](#) in 2023. The government is expected to publish an Anti-Corruption Plan in 2024.

The [ECP2](#) committed the government to decreasing money laundering and increasing asset recovery, tackling kleptocracy and combatting sanctions evasion, reducing fraud, and lowering the threat of international illicit finance to the UK and UK interests. The ECP2 indicated it would



increase resources for law enforcement, expand the National Crime Agency (NCA)'s capacity to fight corruption through its Combatting Kleptocracy Cell (CKC), and support the Crown Dependencies and British Overseas Territories in introducing beneficial ownership registries. It also detailed "cross-cutting system reforms" with a focus on information sharing, data, and technology, boosting law enforcement capacity via a public-private workforce strategy, reforming the criminal justice system, and providing additional funding to the tune of £400 million until the end of the 2025 financial year. A new [Criminal Justice Bill](#), which includes provisions on confiscation, is in Parliament and anticipated in 2024.

The [National Fraud Strategy](#) has three key pillars. The first pillar relates to pursuing fraudsters by boosting law enforcement resources and focusing on intelligence-led disruption. The second pillar focuses on blocking fraud by appointing an Anti-Fraud Champion, calling on the tech sector to stop fraud at an industrial scale, and helping banks slow down suspicious payments. The final pillar is about empowering people through victim support, reimbursement, and raising awareness. The [Payment Services Regulator \(PSR\)](#) issued updates to the Financial Services and Markets Bill, setting out mandatory reimbursements by banks for victims of APP fraud. Requirements will come into force in 2024, and the PSR will detail the level of excess to be paid for claims and guidance on "customer standards of caution." All legal instruments will be available on the PSR website. As part of the ECP2, the UK government has also

been consulting on reform of the [AML/CFT supervisory regime](#). The review, which included an assessment of the Money Laundering Regulations, set out four models to more effectively supervise financial institutions and designated non-financial businesses and professions across England, Wales and Northern Ireland. The reforms were proposed to address inconsistencies and weaknesses in supervision across the UK, including the accounting, legal, and real estate sectors. The consultation results will likely be published in 2024 alongside plans for reform. It is anticipated that updated money laundering regulations will be shared with affected industries in 2024.

Debanking also emerged as a significant regulatory challenge in the UK following allegations of unfair treatment by politician Nigel Farage. The Financial Conduct Authority reviewed the treatment of domestic PEPs and sent a "Dear CEO" letter to banks requesting information on PEP controls. The final [report](#) will be published by the end of June 2024.

The NCA also launched its new Suspicious Activity Report ([SAR](#)) [Online Portal](#) as part of the SAR Reform Program. The objective is to make the SAR reporting regime more effective by allowing firms to submit "structured, meaningful and comprehensive SARs." The NCA also issued [guidance](#) on the new SAR Portal. The NCA released an Amber Alert on using gold to [evade sanctions](#). The UK also recently issued an [Ownership and Control: Public Officials and Control Guidance](#), which applies to the implementation of sanctions.

It is clear now that in the world of AML/CFT, regulations are going to continue to evolve iteratively in response to new risks thrown up by technological innovations, geopolitical events, and increased knowledge of financial crime typologies gained through improved data and information sharing. It can take time for regulatory changes to come to fruition, as some have been signaled for a long time now. Despite this, keeping up with new compliance requirements is a tough ask of firms that are already doing so much in the fight

against financial crime. However, it is imperative that organizations get ahead of this and make use of technologies such as Generative AI that show enormous amounts of promise in the parsing and synthesis of regulatory rules for horizon scanning. Being proactive and having an agile regulatory change process is now critical to ensuring compliance.



Sian Lewin

Founder, The Reg Doctor

China

China will continue fighting illegal financial activity as part of its [“Three-Year Action Plan for Combating Money Laundering Violations and Crimes \(2022-2024\)”](#). In a recent speech by the recently appointed head of the People’s Bank of China (PBOC), Pan Gongsheng, Pan indicated that the central bank would crackdown on fake gold exchanges, third-party wealth management companies, illegal fund-raising, and digital currency transactions. A [crypto ban](#) that was introduced in mainland China in 2021 remains. However, it is estimated that Chinese investors traded [\\$90 billion](#) in crypto in the month of May alone. In response to its FATF Mutual Evaluation Review, China has made various changes to its AML/CFT laws. Risk-based supervision of designated non-financial businesses and professionals has begun with the DPMS regime starting in April 2023. In Hong Kong, the VASP regime under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) extending AML/CFT requirements to crypto exchanges trading non-security tokens went live in June 2023. The [Guidelines on Anti-Money Laundering and Counter-Financing of Terrorism for Authorised Institutions](#) were also amended in May 2023. The [guidelines](#) bring into scope virtual assets and introduce amendments around the use of digital identification systems, more details around beneficial ownership information, clarification of requirements for non-Hong Kong politically exposed persons (PEPs) including risk assessment and ongoing monitoring, prohibitions on anonymous accounts, monitoring of wire transfer requirements, and record-keeping. The Hong Kong Monetary Authority (HKMA) also released a report on [AML/CFT RegTech](#) containing case studies and insights.



Singapore

AML/CFT Review and Corporate Service Providers

The multi-billion-dollar money laundering case in Singapore will continue to drive regulatory changes and reforms in 2024. The government indicated that it would establish an [Inter-Ministerial Committee](#) led by the Ministry of Home Affairs to review the effectiveness of Singapore's AML/CFT framework and identify further measures. The [Committee](#) will focus on preventing corporate structures being misused to launder money, enhancing controls within financial institutions and more effective collaboration to prevent and report suspicious transactions, enhanced AML/CFT measures by real estate agents and corporate service providers, and centralizing and strengthening collaboration across government agencies to tackle money laundering and terrorist financing. Changes have also been proposed to the Accounting Corporate and Regulatory Authority (ACRA) in the CSP Bill, which is anticipated to go live in 2024. The Bill targets Corporate Service Providers (CSPs), also known as Registered Filing Agents (RFAs), and nominee. [Measures](#) include higher penalties for breaches of AML/CFT obligations, including higher penalties by CSPs and fines against persons including directors, owners, partners of CSPs for breaching AML/CFT obligations, introducing requirements for CSPs to screen customers, for CSPs to apply group-wide AML/CFT requirements, provide ACRA with copies of STRs filed with the Suspicious Transaction Office, ensure that nominee directors are fit and proper and adequately trained, and for disclosure by nominee directors and shareholders to disclose their nominee status and identity to ACRA. [Amendments](#) will be made to the ACRA Act and to the Companies Act to introduce these measures.

MAS

The Monetary Authority of Singapore (MAS) will unveil its groundbreaking digital information-sharing platform with the private sector in the [second half of 2024](#) as it seeks to preserve Singapore's reputation as a "safe, trusted and [innovative global financial centre](#)." Provisions for this public-private partnership underpinned by a secure digital platform were introduced by the [Financial Services and Markets \(Amendment\) Bill](#) (FSMB) in May 2023. The Bill sets out

details on how and when the sharing of risk information can take place and includes safeguards to protect the confidentiality of information and the legitimate interests of the customer.

MAS will continue to co-develop the Collaborative Sharing of Money Laundering/Terrorism Financing Information and Cases ([COSMIC](#)) to allow financial institutions "to [warn one another](#) about unusual activity involving their customers" initially with six banks – DBS, OCBC, UOB, Standard Chartered Bank, Citibank, and HSBC. Information sharing will be voluntary initially, and can take place in one of three ways: (1) a bank requests information from another participant, (2) a bank proactively provides information to another, and (3) a bank places a customer on a watchlist to alert other financial institutions. Objective thresholds will need to be met, and MAS will issue a directive detailing threshold criteria and associated "red flags" that correspond to criminal profiles and recognized financial crime behaviors. The thresholds will look to ensure that information sharing is limited to cases of high financial crime concern. The Bill also introduces [protection](#) for participating financial institutions from civil lawsuits, including "granting immunity from liability for any loss arising out of the disclosure on COSMIC, or any act or omission in consequence of the disclosure, if the disclosure was done in accordance with the legal framework, with reasonable care and in good faith." MAS is encouraging customers to respond to CDD requests from banks and has included safeguards in the Bill to protect legitimate customers, such as an independent risk assessment with the available information to avoid sole reliance on information in COSMIC and an opportunity for customers to address bank concerns. Only accurate and complete information can be shared on COSMIC and banks must correct errors and omissions. MAS is also building safeguards to ensure safe use and access to the platform, including strict user access, cybersecurity measures such as data encryption and firewalls to block unauthorized access, and provisions around prohibiting third-party disclosures of information without a court order or request from police. Banks will be required to have strong cybersecurity and encryption controls in place around COSMIC data and will be subject to inspection by MAS. COSMIC will initially focus on identifying the misuse of legal persons, including shell companies, trade-based money laundering, proliferation financing, and sanctions evasion. The platform will be rolled out in [phases](#).

There are a number of additional initiatives that MAS will continue working on into 2024 that are relevant to financial crime prevention compliance teams. These include the ongoing development of regulatory measures for Digital Payment Token (DPT) Services, including cybersecurity measures and consumer protection, a recently launched digital platform to collect and allow access to ESG data, ongoing work with the industry to develop a generative AI risk framework for the financial industry, tackling mobile malware scams and phishing, the expansion of asset tokenization initiatives and the development of foundational capabilities to scale tokenized markets, a regulatory framework for stablecoins, encoding policy and regulatory requirements in protocols for cross-border payments, the use of machine learning to supervise financial institutions in AML/CFT, stronger AML/CFT measures to limit misuse in single family offices. MAS and Bank Negara Malaysia also launched a cross-border real-time payment systems by linking up Singapore's PayNow and Malaysia's DuitNow payment platforms.

The Committee will focus on preventing corporate structures being misused to launder money, enhancing controls within financial institutions and more effective collaboration to prevent and report suspicious transactions

Australia

Australia is expected to [modernize and streamline](#) its exiting AML/CFT framework and introduce Tranche 2 reforms in 2024/2025 to avoid getting added to the FATF grey list. It is estimated that organized crime and illicit financing cost [AUS\\$60.1 billion](#) in 2020 and 2021. The Attorney General announced a consultation on AML/CFT reforms and indicated that the government had accepted recommendations included in the Senate's [Inquiry](#) into the adequacy and efficacy of Australia's anti-money laundering and counter-terrorism financing regime.

Tranche 2 reforms have long been a point of contention in Australia with proposed reforms introduced in 2016 and the Senate publishing a [report](#) in 2022 calling for the inclusion of gatekeepers, or Tranche 2 entities, within AML/CFT regulation. The Senate report included an overview of regulation of Tranche 2 entities, current and emerging challenges in AML, and various recommendations for improvement. Tranche 2 entities include lawyers, real estate agents, casinos, and other gambling service providers, auditors, and dealers in precious metals and stones. Recommendations in the Senate report call for introducing the regulation of gatekeepers and making improvements to the AML/CFT framework. Improvements include simplifying AML/CFT rules, supporting the use of technologies to meet know your customer (KYC) obligations, applying a risk-based approach to regulation, pursuing a beneficial ownership register, increasing penalties for money laundering and terrorist financing, and boosting resourcing in AUSTRAC. The Australian government committed [AUS\\$14.3 million](#) over four years to support necessary legislative and regulatory reforms.

AUSTRAC

AUSTRAC will publish a [national risk assessment](#) on money laundering in early 2024, following the publication of a terrorist financing risk assessment in late 2023. During 2023, AUSTRAC released numerous guidance, including on [de-banking](#), combatting [sexual exploitation of children](#) for financial gain, [employee due diligence](#) and AML/CFT training, customer identification for an [online gambling account](#). From September 29, 2024, [online gambling service providers](#) will need to complete applicable customer identification procedures (ACIP) prior to creating online gaming accounts or providing any designated services.



Crypto Assets

In 2024, Australia is expected to release draft legislation to license crypto asset providers not covered by current regulations for digital assets defined as financial products. In October 2023, the Australian government launched a [consultation](#) on introducing a new regulatory regime for firms providing access to digital assets and custody services for Australians and Australian businesses. It looks to leverage existing financial services laws and regulations to ensure consistency in overseeing and safeguarding consumers. In addition to applying existing obligations,



It is estimated that organized crime and illicit financing cost AUS\$60.1 billion in 2020 and 2021.

proposed new obligations include standard form platform contracts, minimum standards for holding tokens, standards for custody software, and standards to apply when transacting in tokens. Certain digital asset activities, such as trading, staking, tokenization, and fundraising, have also been identified as having [additional obligations](#). Exchanges will have 12 months to comply with the new regime, and businesses providing digital currency exchange services will need to [register with](#) AUSTRAC.

Indonesia

Indonesia will continue to strengthen its AML/CFT laws and regulations as a newly minted member of the FATF. In June 2023, the Indonesian Financial Services Authority (OJK) issued [Regulation \(POJK\) No.8](#) on the Implementation of Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Counter-Proliferation Financing of Weapons of Mass Destruction (CPF) Program in the Financial Services Sector. The regulations will now apply to trusts, securities, crowdfunding, FinTechs, and other financial services firms that fall under the jurisdiction of OJK. It introduced various requirements on proliferation financing, including risk assessment, submission of suspicious financial transaction reports (LTKM), and managing sanctions evasion risk. Firms must also be registered with GoAML to submit reports to the PPAK, Indonesia's FIU. Additionally, it introduced requirements and reminders for firms to develop and submit risk assessments, carry out due diligence - including on beneficial owners - have in place procedures for non-face-to-face verification and requirements for eKYC, revised provisions on compliance functions, internal audits and pre-employee screening and administrative sanctions and requirements to submit data into OJK for supervisory purposes. The regulations came into effect at the end of 2023.



Latin America and the Caribbean

Countries in Latin America will continue to update AML/CFT frameworks to comply with international AML/CFT standards, including bringing VASPs into the scope of regulations and promoting beneficial ownership transparency. Brazil, for example, has published [Federal Decree 11,563/2023](#), which brings VASPs under the purview of the Bacen, the central bank. Bacen will be issuing requirements to comply with AML/CFT laws.

The British Virgin Islands issued [Anti-Money Laundering \(Amendment\) Regulations, 2023](#), clarifying the definition of control, and the Anti-Money Laundering and Terrorist Financing (Amendment) Code of Practice, 2023, which also covers beneficial ownership requirements for trustees, amongst other amendments. [The Virtual Assets Service Providers Act, 2022 \(VASP Act\)](#), which requires VAPs to be registered, became effective on February 1, 2023.

Jamaica introduced the [Companies \(Amendment\) Act 2023 in March 2023](#), creating requirements around the transparency of beneficial ownership and giving powers to the corporate registrar to verify beneficial ownership information. Additional [AML/CFT reforms](#) include allowing information exchanges between national authorities and adopting effective sanctions for non-compliance with BO requirements. Jamaica also set up a new money laundering unit and boosted its IT infrastructure to strengthen its ability to fight financial crime.

The Cayman Islands issued an updated [Proceeds of Crime Act \(2020 Revision\) Anti-Money Laundering Regulations \(2023 Revision\)](#), introducing a myriad of changes around all aspects of the AML/CFT compliance program. This includes the adoption of a risk-based approach and a requirement to risk assess countries and geographies, as well as customer due diligence and additional requirements for PEPs, record-keeping, and reporting. The need to appoint an MLRO is also highlighted, as are identification and record-keeping requirements for wire transfers, identification and record-keeping requirements for virtual assets to comply with the travel rule, measures around correspondent banks, prohibitions for dealing with shell banks, disclosure requirements for persons carrying out relevant financial business, and requirements around DFNBPs, including a duty to maintain a DFNPB register. The Cayman Islands financial regulator CIMA is expected to issue updated AMLRs and AML/CFT guidance.

Countries in Latin America and the Caribbean due to receive a FATF assessment in 2024 include Anguilla, Belize, Guyana, El Salvador, Argentina, Curacao, and Saint Maarten. South American and Caribbean countries on the FATF grey list include Barbados, Haiti, and Jamaica.

Africa and the Middle East

The UAE will continue to carry out changes to make its financial system hostile to ML and TF as it works to get off the FATF grey list, which it was added to in 2022. Since that time, it has taken [various actions](#). It established an Executive Office to Combat Money Laundering and Terrorist Financing to enhance laws and regulations on AML/CFT and created specialized AML/CFT courts to try money laundering and financial crime cases. It also issued new AML/CFT guidelines for financial institutions and designated non-financial businesses and professions. It also adopted the goAML platform to allow financial institutions to file suspicious activity reports. Amendments have been made to the following pieces of legislation:

- AML/CTF Law (Federal Decree Law No. 26 of 2021)
- AML/CFT Regulations (Cabinet Decision No. 24 of 2022)
- Virtual Assets legal framework (Law No. 4 of 2022 Regulating Virtual Assets)

It also adopted a new Penal Code (Federal Decree Law No. 31 of 2021). The Dubai Financial Services Authority (DFSA) updated the AML/CFT and sanctions module of the DFSA Rulebook under the [Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module \(AML\) Instrument \(No. 365\) 2023](#). These changes included an updated [definition](#) of customers and DFNBPs to cover real estate developers or agencies, dealers in precious metals and stones, issuers or service providers for NFTs and utility tokens, law firms, notary firms or independent legal businesses, accountancy and audit firms, alongside insolvency firms or company service providers. The DFSA also indicated that its business plan would focus on monitoring AML/CFT compliance systems and controls, assessing financial crime risks associated with digital assets, and pursuing “fair but firm” enforcement action. [Since 2022](#), the UAE Central Bank has carried out more than 600 inspections, issued ML-related fines totaling more than AED 115 million, and the UAE has seized more than AED 925 million related to AML/CFT breaches. Qatar has published [proposed rules for comment](#), including amendments to the Anti-Money Laundering and Combating the Financing

of Terrorism Rules 2019 and the Anti-Money Laundering and Combating the Financing of Terrorism (General Insurance) Rules 2019. Oman and Kuwait will have their FATF assessments in 2024. Syria, Turkey, and Yemen remain on the FATF grey list.

In efforts to get off the FATF grey list, both South Africa and Nigeria will continue to reform their AML/CFT regulations. In [South Africa](#), the president signed into law the following pieces of legislation in late December 2022:

- [General Laws](#) (Anti-Money Laundering and Combatting Terrorist Financing) Amendment Act No. 22 of 2022 amending:
 - » Trust Property Control Act, 1988
 - » Nonprofit Organisations Act, 1997
 - » Financial Intelligence Centre Act, 2001
 - » Companies Act, 2008
 - » Financial Sector Regulation Act, 2017
- [Protection of Constitutional Democracy against Terrorism and Related Activities \(POCDATARA\)](#) Amendment Act No. 23 (effective 4 January 2023) of 2022 amending:
 - » Protection of Constitutional Democracy Against Terrorism and Related Activities Act, 2004

The General Laws Amendment Act enhances the requirement to perform due diligence, creates transparency around the beneficial ownership of corporate vehicles, including trusts and companies, creates a regulatory framework to protect NPOs from being misused to finance terrorism, and introduces fit and proper requirements for beneficial owners of financial institutions. The POCDATARA Amendment Act refines the definition of the terrorist financing offense, includes cyber-terrorism, and allows for financial sanctions against supporters of terrorist organizations. South African authorities also developed a national strategy to address remaining deficiencies with FATF standards.

The [Central Bank of Nigeria \(CBN\) issued the Central Bank of Nigeria \(Customer Due Diligence\) Regulations](#) in June 2023. The regulations prohibit anonymous accounts and detail additional due diligence measures, including requirements around identifying and verifying the beneficial owners of legal persons and legal arrangements, the nature and purpose of business, and e-KYC. It also details a risk-based approach to CDD, enhances CDD measures, and provides additional measures, including external non-resident, non-Nigerian accounts. It introduced sanctions for non-compliance.

Several African countries will have their FATF assessments in 2024. These include Equatorial Guinea, Eritrea, Comoros, Djibouti, and Sao Tome & Principe. Burkina Faso, Cameroon, the DRC, Mali, Mozambique, Senegal, South Sudan, Tanzania, and Uganda remain on the FATF grey list. Burkina Faso, Cameroon, Mali, Niger, and Nigeria, which are part of the Sahel, continue to face violence, terrorism, and humanitarian crises making AML/CFT reforms challenging. South Sudan's progress with complying with FATF standards may also be affected if violence erupts in 2024 due to anticipated elections.



What does this mean for my firm?

Many pieces of legislation and regulation are being updated around the world as AML/CFT increasingly becomes a national security issue. This makes it even more important that they have dedicated resources to manage their regulatory risk exposure. Compliance leaders should also be monitoring global developments as part of horizon planning to identify any potential future demands on their business and consider incorporating best practice into operations where it is possible to do so.

Firms should assess whether laws impact their businesses directly and/or indirectly depending on whether branches and subsidiaries operate in jurisdictions with legal and regulatory changes. Impact and regulatory gap assessments alongside action plans are important to ensure relevant updates are rolled out. Firms should then update internal policies, procedures, and systems to align with new laws and regulations and identify staff that will be affected.

Training should also be updated to reflect changes to internal policies, processes, and systems.

Finally, records of key changes should be maintained, and where senior management is required on updated policies and procedures, this should be obtained by financial crime compliance departments.



Andrew Davies

Global Head of Regulatory Affairs,
ComplyAdvantage

[↑](#) Back to beginning

[←](#) Previous section



Regulatory themes

Artificial Intelligence

As financial crime professionals continue to explore the efficiencies offered by artificial intelligence (AI), policymakers will continue to focus on mitigating what leaders have described as the [existential threat](#) some argue these technologies pose. The [FATF](#) has addressed the use of AI, citing the need for governance to ensure appropriate oversight, explainability to avoid a 'black-box' approach, and model performance to ensure ongoing monitoring for valid outcomes. There are also several international initiatives that firms need to be aware of. During the G7 in Hiroshima in May, leaders indicated a determination to work together on inclusive AI governance and interoperability. The Organization for Economic Cooperation and Development (OECD) subsequently published a [stocktake](#) of AI to create a common understanding of generative AI as part of the 'G7 Hiroshima Process on Generative AI'. Key priorities for G7 countries include:

- Human rights;
- The security of systems;
- The preservation of democratic values;
- Privacy and data governance;
- The safety of people;
- Alignment of AI objectives and human values;
- Inclusion;
- Lack of bias;
- and explainability (amongst others).

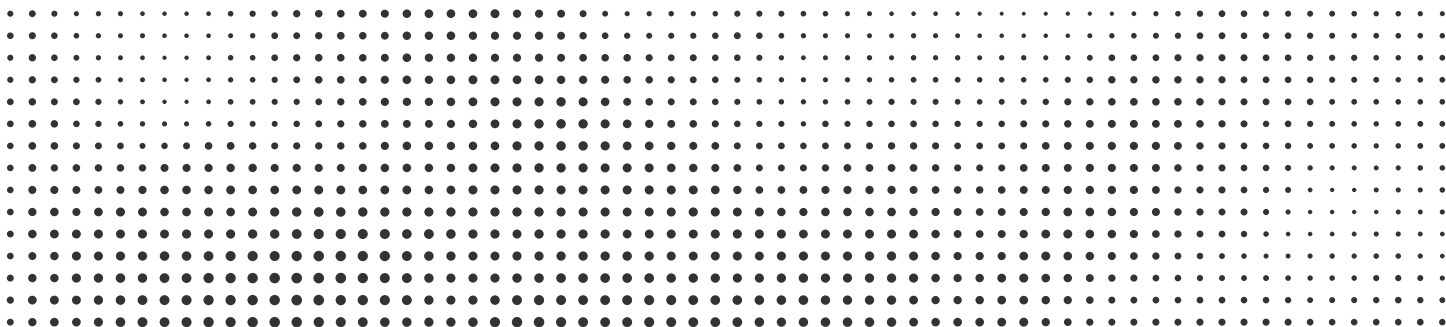
In October, the G7 issued a Statement on the Hiroshima [AI Process](#), announcing the Hiroshima Process International [Guiding Principles](#) for Organizations Developing Advanced AI System and the Hiroshima Process International [Code of Conduct](#) for Organizations Developing Advanced AI Systems to address identified priorities.



In November, the United Kingdom brought together government and technology leaders with twenty-eight governments, including the UK, US, EU, Australia, and China, aggregating to the [Bletchley Declaration](#) on AI safety. The declaration highlights the need for international cooperation to address risks associated with AI to harness the “[transformative positive potential of AI](#)” while ensuring the development of human-centric, trustworthy, and responsible AI. Companies also agreed to [test new models](#) with governments before they are released to manage risks.

Crucially for AML/CFT professionals, regulators, and policymakers are beginning to sketch out how AI could be regulated nationally. The EU is leading the way with the [EU Artificial Intelligence Act](#), which promotes a [risk-based approach](#) to regulating AI with more stringent requirements for higher-risk AI systems. It introduces different risk levels and the need to categorize these under headings such as an unacceptable risk considered to be a threat to people. A high-risk use case, for example, may affect people’s safety or fundamental rights. It also creates a special category for generative AI. The Act also introduces new transparency obligations for AI systems, such as notifying humans that they are interacting with an AI system and applying labels to deep fakes alongside voluntary codes of conduct for low-risk AI systems. It also details certain obligations for operators and around using biometrics for law enforcement purposes. The AI Act looks to harmonize regulatory approaches to AI, is likely to be adopted in [early 2024](#), and will have a transition period of 18 months. The AI Act also introduced penalties for miscategorizing AI systems or the relevant requirements up to €20 million or 4 percent of global turnover. The AI Act should be considered alongside other measures, including the [General Data Protection Regulation](#), the [Digital Services Act](#), and the [Digital Markets Act](#). The EU is also reviewing its [Strategic Plan for Artificial Intelligence](#), which is due to be updated by 31 December 2023.

AI legislation remains relatively new in the US, with numerous federal and state initiatives. White House initiatives include an agreement on [voluntary AI commitments](#) with some of the world’s biggest tech companies, a [Blueprint for an AI Bill of Rights](#) to protect against algorithmically generated harmful bias and data privacy, an updated [National AI R&D Strategic Plan](#), and an [Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence](#). The Executive Order is designed to create new AI safety and security standards, protect privacy, advance equality and civil rights, stand up for consumers, support workers, and promote innovation and competition. It also protects consumers against fraud by creating standards for identifying AI-generated content and authenticating official content. The US published an [AI Risk Management Framework](#) which describes how firms should manage the risks of AI systems. Both the Financial Crimes Enforcement Network ([FinCEN](#)) and the Office for Foreign Assets Control ([OFAC](#)) have previously signaled to the private sector that they welcome the use of AI in financial crime prevention, sanctions management, and instant payment systems. The US has further issued guidance and business advisories and frameworks to promote safety, security, and trust in the future development of responsible AI. At the state level, laws currently enacted relate to data protection, profiling, and automated decision-making and require impact assessments to detect high-risk activity to consumers. The laws also cover various topics and set precedents for future AI regulation. This includes topics such as consumer protection, user data and security, the use of bots, preventing bias, and requirements around the use of automated decision systems (ADS) for monitoring employees to protect the safety of employees.



Canada is expected to approve a proposed [Artificial Intelligence and Data Act \(AIDA\)](#) and supporting regulation, including a risk-based regulatory framework promoting the responsible design, development, and use of AI systems around 2025. The UK published a [National AI Strategy](#) in December 2022 and will continue to assess the scale and size of gaps in existing mitigation measures to manage risks. The UK also issued a [whitepaper](#) outlining a pro-innovation approach to AI regulation, including exploring the development of an AI regulatory sandbox. Japan will continue to apply existing frameworks, including the Penal Code and enforcement action and existing guidelines, including the AI R&D Guidelines, the AI Utilization Guidelines, the [Social Principles of Human-Centric AI](#), and the [Government Guidelines for the Implementation of AI principles](#). It will also consider integrating and revising guidelines into a single source for different types of users. China is said to be issuing “[groundbreaking new strategies](#)” to govern AI, including regulations on algorithms, rules for deep synthesis (synthetically generated content), and draft rules on generative AI, which requires training data and model outputs to be ‘true and accurate,’ with developers required to register with China’s algorithm registry and to pass a security self-assessment. The various pieces of legislation being introduced will likely have implications for regtech and the development and use of AI financial crime prevention solutions. This includes using facial recognition as part of onboarding and automated decision-making and profiling around risk assessments, triaging of alerts and matches during adverse press and sanctions screening, and transaction monitoring solutions using AI. There is also an ongoing focus on the concept of explainability, where firms must be able to show that they understand how the algorithm makes decisions.

What does this mean for my firm?

Firms should familiarize themselves with the obligations and guidance issued as they specifically apply to the use of automated systems, bias, and data privacy. They should also ensure they have adequate documentation detailing risk assessments and risk management processes for AI, model governance, model testing and validation, and how the algorithm makes decisions to account for explainability. When training AI models, firms should ensure that they use data from multiple sources, covering all demographics and from across geographies, to avoid bias. Finally, compliance teams should ensure that they have senior management support, carry out due diligence on vendors, and ongoing monitoring and assurance.



Iain Armstrong

Regulatory Affairs Practice Lead,
ComplyAdvantage

Real-Time Payment Schemes

As real-time payment schemes are increasingly adopted and the world transitions to ISO20022, the focus will remain on promoting transparency and managing risk. The World Bank monitors the implementation of [fast](#) (instant, real-time, immediate, rapid) payment systems worldwide. Its data suggest that Europe and Central Asia have the greatest access to faster payment systems and that India, the UK, and Nigeria have processed the highest annual volume of payments. 87 percent of countries apply the ISO20022 messaging standard, and 84 percent have open-access APIs. The World Bank has also published reports on fraud risks in fast payments alongside approaches and challenges for customer authentication. The [fraud report](#) includes typologies, lists fraud prevention techniques such as the importance of education, regulation, scheme rules, and technology, and details case studies from around the world. The [authentication report](#) provides an overview of different authentication approaches, such as factor-based authentication, digital identity-based authentication, and risk-based authentication, as well as best practices and considerations to consider, such as inclusion, user experience, privacy concerns, and the roles of various actors.



What is ISO20022?

ISO20022 is an open global standard that promotes harmonization and is expected to support greater transparency in payments, making transaction monitoring and screening more effective, particularly for real-time payments.

Global payment messaging provider SWIFT encourages instant and real-time gross settlement systems to adopt the ISO20022 “to align with the richer format of cross-border payments.” Migration to the new standard in SWIFT started in March 2023, and SWIFT will maintain MT message types to allow firms to get onto the new standard until November 2025. It is anticipated that by 2025, [approximately 80 percent of payments worldwide will be processed on ISO20022-compliant rails](#), making that the global standard for payment messaging. ISO20022 will also bring greater efficiencies in AML/CFT compliance, with structured, labeled data reducing false positives, requests for information, and friction. [Key areas](#) that will be impacted include screening for sanctions, PEPs and adverse press, transaction monitoring, and fraud monitoring. Regarding sanctions screening, it is anticipated that ISO20022 will include a higher volume of more accurate data, reducing false positive rates. For transaction monitoring, ISO20022 will provide additional remittance data, such as debtor and creditor information, to help identify new typologies. It is anticipated that the higher quality data provided in ISO20022 payments will make it easier to identify fraudulent payments in real time, helping to tackle complex fraud.

More widely, European policymakers continue to drive the adoption of real-time payments across the continent. The European Central Bank previously introduced the [SEPA Instant Credit Transfers Scheme \(SCT Inst\)](#) for processing payments in less than ten seconds. The European Payments Council published an updated SPEA Instant Credit Transfer [rulebook](#) listing the new implementation date as March 17, 2024. Unfortunately, access to instant payments is not consistent across all SEPA jurisdictions. In November 2023, the European Council and Parliament reached a [political agreement](#) on instant payments, including introducing [uniform rules](#) for cross-border instant credit transfers and new rules to reduce reliance on third-country financial institutions. The new rules also have a requirement for providers to verify a match between the beneficiary’s IBAN and name to identify potential fraud or mistakes before a transaction is made.

There has been limited adoption of real-time payments in the US, accounting for 1 percent of payments nationwide. The Federal Reserve is rolling out the [FedNow Service](#) to promote the adoption of instant payments. FedNow went live in July 2023 and allows eligible depository institutions to offer instant payment

services 24 hours a day, seven days per week. The service carries out interbank clearing and settlement, allowing payments to be transferred in near real-time. The FedNow Service has optional fraud prevention [tools](#), the chance to join as a ‘receive-only participant,’ ask for payment capabilities, and tools to help those participating in the scheme handle payment inquiries. The FedNow service will apply ISO20022 principles to enhance payment speed, traceability, and transparency. Since 2021, over 57 organizations have signed up as early adopters, including JPMorgan, Chase, BNY Mellon, and US Century Bank. Firms must complete testing and certification to use the payment rail and confirm that they comply with ISO20022 standards. Concerns remain that instant payment systems will attract fraudsters. FedNow has indicated that its suite of fraud prevention and detection tools will evolve.

What does this mean for my firm?

Firms must review legislation and guidance and work with their IT departments to fully understand and adopt new requirements (both legal, regulatory, and technical standards) to adopt real-time payments. They should ensure that related payment processes and policies are updated to reflect changes introduced by ISO20022 and that data is clean and accurate before feeding into the system.

Compliance leaders should also ensure that their staff are adequately trained to act on new message standards and understand the impact of adopting ISO20022. Firms need to ensure they calibrate existing systems and controls as they integrate the new payment format to ensure that they remain fit for purpose with more data available for screening

Firms will also need to have strong transaction screening and fraud detection systems in place and must be able to educate their customers to help them identify when fraudsters are targeting them.



Andrew Davies

Global Head of Regulatory Affairs,
ComplyAdvantage

Beneficial Ownership and Corporate Transparency

Beneficial ownership and corporate transparency will remain key in the fight against financial crime, and more countries will continue to explore launching or reforming their beneficial ownership registries.

In our State of Financial Crime 2024 survey,

40%

of firms said UBO legislation was an area of AML regulation that could be tightened to combat financial crime in their countries effectively – the third-highest answer given.

The Financial Action Task Force (FATF) announced in October 2023 that it is developing risk-based guidance on beneficial ownership and transparency of legal arrangements for publication in February 2024. The guidance will be updated to align with revisions made to Recommendation 25 and to complement the guidance on legal persons to help those working in trusts and legal arrangements better assess and mitigate financial crime risks.

Source: ComplyAdvantage, *The State of Financial Crime 2024*

The European Union (EU) has faced major challenges in implementing public beneficial ownership registries as stipulated by the 4th and 5th Money Laundering Directives. This is due to a November 2022 [judgment](#) by the Court of Justice of the European Union (CJEU), which found that public access to beneficial ownership registers “constitutes a serious interference with the fundamental rights enshrined in Articles 7 and 8” of the General Data Protection Regulation. The judgment highlighted that press and civil society organizations that counter money laundering and terrorist financing “have a legitimate interest in accessing information on beneficial ownership.” This led to countries taking down public beneficial ownership registries. Countries in the process of implementing beneficial ownership registries include Hungary, Italy, Lithuania, Norway, and Switzerland. In [Switzerland](#), the Federal Council is looking to develop a beneficial ownership register that will likely cover foreign entities operating in Switzerland and beneficial owners holding more than 25 percent and persons exercising “substantial control.” It will only be accessible to law enforcement and will be managed by the Federal Department of Justice and Police.

In the US, the [Corporate Transparency Act \(CTA\)](#) requires businesses to maintain a record of their shareholders or ultimate beneficial owners (UBOs) and disclose information to FinCEN, who will make it available to law enforcement. A [beneficial owner](#) is an individual who owns or controls (directly or indirectly) at least 25 percent of the ownership interest. The CTA applies to US entities and foreign entities doing business in the US. Requirements include collecting a full name, date of birth, current address, and a distinctive identification number. Businesses will need to update FinCEN with any material changes. New reporting requirements will come into effect on January 1, 2024, with companies that are already established required

to share UBO information with FinCEN by January 1, 2025, and companies established after January 1, 2024, required to share information with FinCEN within 30 days. Failure to comply could lead to civil penalties of \$500 per day (up to \$10,000) and up to two years imprisonment. FinCEN has issued [Beneficial Ownership Information Reporting Guidance](#), including FAQs, key filing dates and key questions, and a [Small Entity Beneficial Ownership Information \(BOI\)](#) guide to help companies comply with the CTA.

Canada is in the process of implementing a public beneficial ownership registry. The UK also recently introduced new requirements and powers under the [Economic Crime and Corporate Transparency Act \(ECCTA\)](#) to address concerns around the misuse of its national corporate registry, Companies House, to set up companies to launder the proceeds of crime and support illicit activities. Companies House has been criticized for failing to verify the names and addresses provided when setting up a company, allowing organized crime groups from abroad and oligarchs to hide their money in the UK. New [identification requirements](#) will apply to directors and ‘People with Significant Control, and registration will be required via Companies House or through an Authorised Corporate Service Provider (ACSP). A new beneficial ownership register will also be introduced. ACSPs will need to keep identity verification records. Individuals can request certain information to be suppressed on the register to [prevent the abuse of personal information](#).

[Open Ownership](#) publishes a map of worldwide action on beneficial ownership transparency. Around the world, there are 63 live beneficial ownership registers, with 18 countries in the process of implementing beneficial ownership registers and 51 planning to implement beneficial ownership registers.

What does this mean for my firm?

Businesses should ensure they can comply with new beneficial ownership rules as they emerge in different countries. They should seek legal counsel, invest in Know Your Business (KYB) compliance tools and training, and stay informed about updates to national legislation and related regulations on beneficial ownership. Finally, compliance leaders should ensure

that they carry out comprehensive due diligence, including identifying and verifying beneficial ownership information as required by local law.



Iain Armstrong

Regulatory Affairs Practice Lead,
ComplyAdvantage

Continued Growth of Public-Private Partnerships

Public-private partnerships (PPPs) will continue to grow and evolve, incorporating new technologies in some jurisdictions to tackle different aspects of financial crime. Although different models exist, with both formal and informal PPPs popping up worldwide, they will continue to yield unique insights and lead to better results in tackling economic crime. At a global level, a recent [Global Advisory](#) on Russian Sanctions Evasion issued by the Russian Elites, Proxies, and Oligarchs (REPO) Task Force included a recommendation for regulated and non-regulated firms to “take part in existing public-private partnerships.” This recognizes their unique role in the international financial system and their access to valuable data and insight. Benefits include hearing from competent authorities on Russian sanctions while allowing other authorities to learn more about risks, trends, and typologies seen by the private sector.

At the national level, the Monetary Authority of Singapore (MAS) is working with the private sector to build a groundbreaking digital information-sharing platform called the Collaborative Sharing of Money Laundering/Terrorism Financing Information and Cases ([COSMIC](#)). Provisions to develop an electronic information-sharing system were introduced by the [Financial Services and Markets \(Amendment\) Bill](#). COSMIC is being developed with six banks – DBS, OCBC, UOB, Standard Chartered Bank, Citibank and HSBC – to share information when red flags are identified securely. COSMIC will initially focus on identifying the misuse of legal persons, trade-based money laundering, and proliferation financing. It will be rolled out in phases beginning in the second half of 2024.

The UK was one of the first countries to establish a PPP, the Joint Money Laundering Intelligence Task Force (JMLIT). It will continue to explore more public-private partnership collaboration in the fight against economic crime. In 2023, the [Economic Crime and Corporate Transparency Act \(ECCTA\)](#) unveiled new tools to facilitate PPPs and information sharing. [Measures](#) introduced include allowing

for direct data sharing between regulated businesses and indirect information sharing through third-party intermediaries. The [2023-2026 Economic Crime Plan](#) also includes actions to promote greater public-private collaboration. This includes establishing a public-private cell to strengthen the response to emerging risks associated with crypto, creating a new Public Private Economic Crime Data Strategy to go after financial crime, and developing a public-private workforce strategy to promote greater collaboration and skill-sharing between the public and private sectors.

The US also has a long-standing history of public-private intelligence sharing. The FinCEN Exchange was established under section 6103 of the Anti-Money Laundering Act of 2020 to develop a collaborative investigative model that operates under section 314(b) of the USA PATRIOT Act. In 2023, it held meetings with financial institutions to combat [fentanyl trafficking](#), [human smuggling](#), the [DPRK's illicit cyber activities](#), and [cyber-related terrorism financing](#). Other public-private information-sharing collaborations include Estonia's Salv-AML Bridge, Switzerland's AML Utility, the Netherlands' Transactie Monitoring Nederland (TMNL), and Australia's Fintel Alliance. The Fintel Alliance published its [2023 report](#) citing successes, including tackling money mules, the illegal exportation of waste tires, the illegal wildlife trade, disrupting terrorism and professional money laundering, and child sexual exploitation.

With regards to other PPPs, [Mexico](#) is in the process of establishing a financial intelligence-sharing partnership with business and government leaders coming together in 2022 and 2023 to discuss how to address Mexico's national security and financial crime concerns. In early 2023, South Africa's FIU SAMLIT partnered with a data company and worked with multiple banks to identify financial flows and indicators to tackle modern slavery and [human trafficking](#), leading to the development of new typologies and the identification of key insights that were unknown allowing the FIU to make more targeted policy and resourcing decisions.

What does this mean for my firm?

“ In our State of Financial Crime 2024 survey,

56%

of firms said they're already involved in a public-private partnership, with another 39 percent intending to join within the next 12 months. This is really encouraging, given the outsized impact these groups can have across various areas.

To maximize the opportunity, firms should identify local public-private partnerships and explore how to engage local FIUs. Where joint advisories are published by public-private partnerships, firms should identify how to build findings into relevant risk assessments, policies, and systems to ensure that they can identify emerging threats.

”

Alia Mahmud

Global Regulatory Affairs Practice
Lead, ComplyAdvantage

Circumventing Sanctions

As countries continue to apply complex sanctions to increase the costs of Russia's war in Ukraine, sanctions circumvention will remain a key area of regulatory focus. While there has been a growth in the scope and maturity of sanctions programs, there have been concerns that although sanctions have contributed to a shrinking economy in Russia, they may not be having their full intended effect due to sanctions circumvention. A report analyzing customs data highlighted that around [\\$8.5 billion](#) was linked to the circumvention of export sanctions on Russia. While exports to Russia from Western countries decreased significantly, exports, including dual-use products, increased significantly to neighboring countries such as Azerbaijan, Kazakhstan, Georgia, Armenia, Kyrgyzstan, Turkey, and Belarus. These [third countries](#) have been used to re-export goods to sell products into Russia, with exports [skyrocketing](#) in electronic equipment, vehicles, machinery, and nuclear reactors. [Electronics exports](#) from Armenia to Russia increased by 3,700 percent between 2021 and 2022. Countries such as Turkey, Serbia, and Kazakhstan were also identified as providing [semiconductors](#) to Russia. The Russian Elites, Proxies, and Oligarchs (REPO) Task Force, which consists of Australia, Canada, the European Commission, France, Germany, Japan, Italy, the UK, and the US, are leading the way in fighting sanctions circumvention. In March 2023, the REPO Task Force released a statement

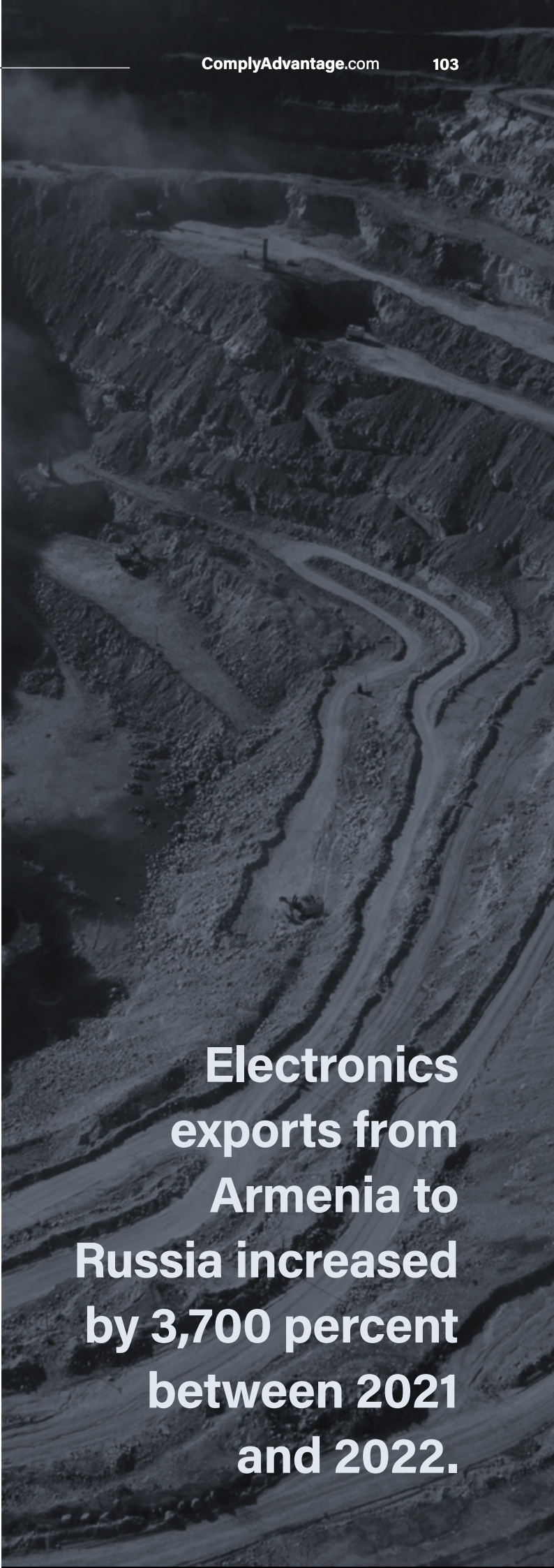
highlighting that its members had successfully blocked or frozen over [\\$58 billion](#) of sanctioned assets. It shared steps taken, including working together to investigate and counter sanctions evasion by Russian actors looking to launder funds or use crypto assets and financial facilitators to hide or obfuscate assets. It called on "the international community to join these multilateral efforts to counter Russian sanctions evasion and circumvention attempts," and members jointly issued a [Global Advisory on Russian Sanctions Evasion](#). The advisory highlighted the following typologies:

- The use of family members and close associates to maintain access and control of wealth and companies.
- The use of real estate to hold value and benefit from wealth.
- The use of complex ownership structures to avoid identification.
- The use of enablers to avoid involvement and leverage expertise.
- Use of Third-Party Jurisdictions and False Trade Information to Facilitate Sensitive Goods Shipment to Russia.



It calls on regulated entities to take further measures that firms should be aware of. Measures include complying with global AML/CFT rules, reviewing AML/CFT compliance programs, participating in public-private partnerships, leveraging information-sharing protocols, updating risk assessments, and increasing awareness of sanctions risk and impact for entities not subject to AML/CFT regulations. Following its most recent meeting in September 2023, the REPO Task Force revealed that it had mapped out [Russian sovereign assets](#) held in REPO countries, which amounted to \$280 billion, much of it in the EU. The Financial Intelligence Units of the G7, alongside the Netherlands, Australia, and New Zealand, have also created the [Russia-Related Illicit Finance and Sanctions \(RRIFS\)](#) working group to share financial trends and reports sharing indicators of Russia-related sanctions evasion.

The EU will issue regional sanctions, and individual countries will also continue to apply unilateral sanctions against companies and persons evading sanctions. The EU announced its 12th sanctions package which is expected to target Russian rough and polished diamonds and focus on sanctions evasion measures. The 11th package targeted Chinese companies suspected of circumventing sanctions. The EU has also published [guidance against sanctions circumvention](#) requiring the assessment of risks, the design and implementation of mitigating measures, and the need to keep these up to date as threats evolve. The guidance also provides good practices for carrying out enhanced due diligence, best practices to address potential sanctions circumvention, and a list of red flags related to business partners and customers. The US, UK, and EU have also taken steps to target the Russian diamond industry, which has previously generated \$4 billion in revenue for Russia. In [February](#) and [November](#), the US sanctioned 30 third-country individuals and companies connected to arms trafficking and illicit finance with links to Switzerland, Malta, Bulgaria, Cyprus, the US, and the UAE. FinCEN has issued previous alerts citing sanctions evasion measures by using [corporate vehicles and shell companies](#) and [luxury goods or other high-value assets](#) in March and the need for greater vigilance to identify [export control](#) evasion. The [Department of Justice](#) has indicated it is investigating sanctions evasion by corporate operations in the transport, FinTech, banking, defense, and agriculture industries. The UK recently released a [Red Alert on Gold-based Financial and Trade Sanctions Circumvention](#), citing common circumvention techniques, typologies for circumventing the 2022 gold import ban, and risk indicators for mined gold, recycled/scrap gold,



**Electronics
exports from
Armenia to
Russia increased
by 3,700 percent
between 2021
and 2022.**

investment gold, and gold for jewelry. The UK's [Export Control Joint Unit \(ECJU\)](#) also published risk indicators for the diversion of goods for the evasion of trade sanctions, and the FCDO has identified high-priority items used by Russia for its weapons system at risk of sanctions evasion. The FCDO and OSFI recently issued [guidance on ownership and control](#) to prevent sanctions circumvention.

Russia, however, will continue to adapt and explore other currencies and markets to prop up its economy. To work around the [oil price cap](#), Russia has begun working with, according to analysts, "little-known trading firms with no history in the business, popping up and exporting large volumes of Russian crude exports to Asia and then closing business rapidly" alongside a fleet of hundreds of small taker operators operating aging 'shadow tankers' under Liberian or Cameroonian flags. These tankers pose huge environmental risks and often lack insurance. Oil exports have also been redirected to China, India, and Turkey. India has emerged as the world's second-largest purchaser of Russian crude, increasing imports from 1 percent before the war in Ukraine to 40 percent and generating [savings](#) of \$2.7 billion by importing discounted Russian crude. Oil products have made their way back to Europe from India and Turkey.

Russian imports are also increasingly invoiced in [yuan](#), accounting for 63 percent of imports from China in 2022, and other countries such as Mongolia and Tajikistan have a currency swap line with the People's Bank of China.

Another focus of sanctions evasion is North Korea's circumvention of UN sanctions. The G7 [appealed to China](#) to stop sanctions evasion measures of the petroleum and oil cap imposed in 2017. In July, a letter issued to the Chinese government cited concerns "regarding the continuing presence of multiple oil tankers ... that use your territorial waters in Sansha Bay as refuge to facilitate their trade of sanctioned petroleum products to the DPRK." The letter included satellite imagery showing that sanctions evasion practices "continued into 2023." The UN has added vessels to its blacklist for evading sanctions.

What does this mean for my firm?

Firms should review all local guidance, business advisories, and alerts in the countries in which they operate and ensure that they are building relevant measures into sanctions and AML/CFT compliance programs.

They should also ensure to carry out enhanced due diligence, including supply chain due diligence measures when dealing with oil, gold, and other commodities subject to complex sanctions. Compliance teams should regularly update their risk assessments, carry out screening and payment filtering, and calibrate systems to identify new modes and methods of sanctions circumvention as they emerge

Finally, firms should ensure that members of staff are adequately trained on sanctions evasion techniques and that ways of reporting sanctions evasion are clear and accessible to staff.



Alia Mahmud

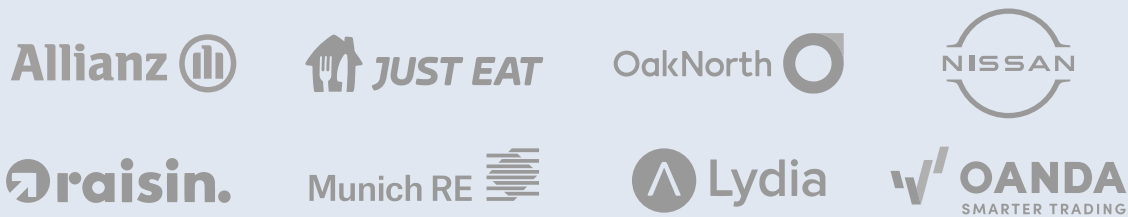
Global Regulatory Affairs Practice
Lead, ComplyAdvantage

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

EMEA

London

+44 20 7834 0252
[Demo Request](#)

AMER

New York

+1 (646) 844 0841
[Demo Request](#)

APAC

Singapore

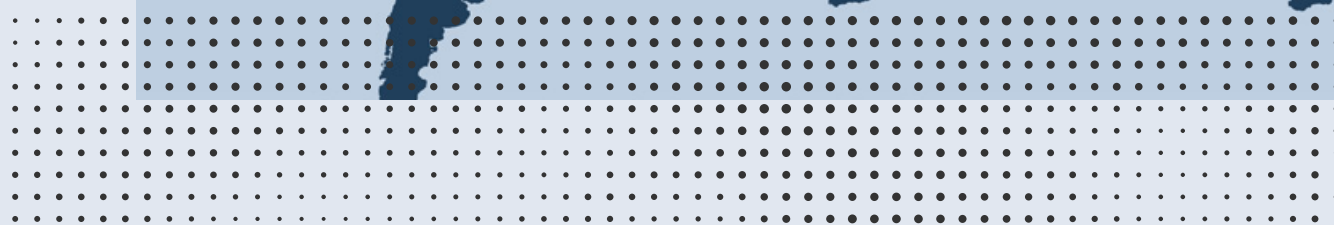
+65 6304 3069
[Demo Request](#)

Survey Methodology

The State of Financial Crime 2024 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, with 50+ employees and total assets worth \$5 billion+.

600



Disclaimer: This is for general information only. The information presented does not constitute legal advice. ComplyAdvantage accepts no responsibility for any information contained herein and disclaims and excludes any liability in respect of the contents or for action taken based on this information.

