COMPLY ADVANTAGE®

The

State of Financial Crime

2023

Contents

Introduction

Andrew Davies
Global Head of Regulatory Affairs,
ComplyAdvantage

2023 was supposed to be the year we escaped the shockwaves of the COVID-19 pandemic. It's clear from this year's survey that won't be the case.

The global economic crisis triggered by the inflationary effects of the 'return to normal' and the war in Ukraine drove a whopping 99 percent of respondents to tell us they're re-evaluating their risk appetite in 2023. It's pleasing to see 58 percent of compliance teams are planning to hire in 2023 to meet this challenge. Most respondents also showed they understand that preventing and managing financial crime risk is not just a question of hiring more people - technology and organizational transformation are also critical. Financial inclusion could be severely impacted unless appropriate technology is used to optimize the onboarding process for reimagined risk appetites.

Our report highlights other key areas - including financing terrorist groups through decentralized platforms - where long-standing trends accelerated through the pandemic. Environmental crime is another major theme, with crimes like poaching and illegal logging on the rise too.

The invasion of Ukraine and its continued global impact remain another central theme for the year ahead. Unsurprisingly, Russia became the geopolitical hotspot firms are most concerned about, overtaking China. With no prospect of a resolution in sight, the focus will remain on an unprecedented sanctions regime that could become a blueprint for future crises. For now, we expect sanctions on Russia to tighten further in 2023, despite the intense pressure many Western countries are facing through sky-high energy and food bills. We should also expect an increased focus on familiar hotspots, including North Korea and Iran.

On the regulatory front, we expect to see the first fruits of the Financial Action Task Force's (FATF) Singapore presidency, with asset recovery a key focus. In the United States, we will see major regulatory reform of the crypto asset market, though much remains undecided. China and Singapore have also made important strides in regulating virtual asset service providers. Meanwhile, the European Union's (EU) continued program of AML reform is likely to become law, creating a new Anti-Money Laundering Authority (AMLA) for the bloc.

The final section of our report considers wider industry trends and themes. This year, we explore the ongoing focus on beneficial ownership and corporate transparency and their importance for understanding factors including source of funds, corruption, and tax evasion. Firms also told us which artificial intelligence (AI) use cases add the most value. Lastly, Know Your Business (KYB) and environmental and social governance (ESG) initiatives will take center stage in 2023. We break down the practical implications of this shift for the compliance community.

The stakes are incredibly high, from an entrenched war in Europe to the most volatile global economic environment for over a decade. The challenges facing compliance professionals have arguably never been more complex. Yet I remain optimistic. The tools, technologies, and guidance available to firms are better than ever, which means more effective financial crime-fighting and - ultimately - a better world for all of us.

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

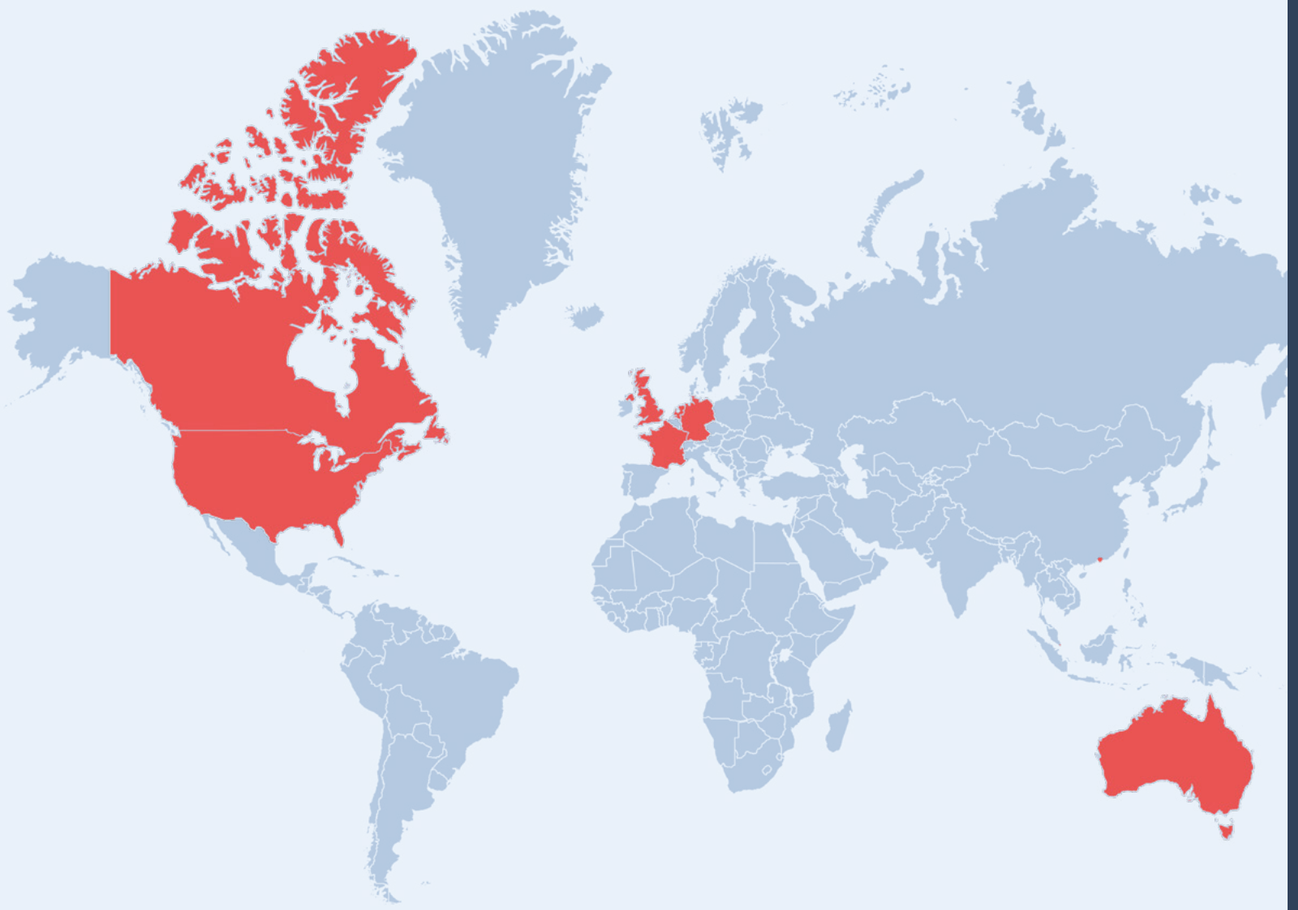
Best Wishes,

Methodology

This report is based on a survey of 800 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+.

The sectors covered in interviews are financial institutions (e.g., banks), digital banking & fintech, wealth management, investment (retail), capital markets, money service businesses, crypto exchanges, and insurance.



← Back to contents

Next section →

Spotlight on Financial Crime

This section explores the trends shaping today's financial landscape and their implications for the year ahead. As our survey shows, for 2023, firms are bracing for a rise in financial crime, and as a result, they're staffing up and rethinking their approach to risk.

The change that has attracted the most comment, however – and has had the most significant impact on obligated entities – has been the introduction of 'aiding and abetting' as an offence. This is an attempt to deter the growth of the market for professional enablers of money laundering in the legal, accountancy and professional services sector, but also amongst the family members, friends and associates of criminals who played roles as proxies in complex laundering schemes. In practical terms, the 'aiding and abetting' offence means that anyone - and that includes businesses as well as individuals (see 'Liability' below) - who help money launderers hide funds could themselves be committing the crime of money laundering.

However, as many in the industry asked at the time of the directive's introduction, it was not clear what the application of 'aiding and abetting' would mean in practice. Where an advisor or financial institution had explicitly known or even surmised that funds were criminally generated, but how allowed this to proceed, this would be an offence. But what of 'acts of omission'? The risk exists that prolonged unintentional compliance failures, allowing criminals to launder funds, might be deemed a criminal act, as well as a regulatory failure requiring enforcement action.

Economic volatility is reshaping attitudes to risk

The global economic downturn will disrupt the financial crime and compliance space in 2023. While some commentators had predicted a 'roaring twenties' as much of the world reopened and the "Great Resignation" reshaped workplaces, the reality has proven sobering.

99 percent of organizations globally told us they're re-evaluating their risk appetite due to the economic environment. 57 percent are doing so "to a great extent." This more conservative approach, and the additional customer due diligence it will require, is set to pile further pressure on the expectation that access to financial services is slick and frictionless. Meeting this demand while managing tougher risk appetites will require investments in both technology and staff.

Underlying industry caution is an expectation that, as in previous economic downturns, levels of financial crime will increase. This may not entirely come from hardened professional criminals, either. Economic pressure is likely to drive a wider increase in risk-taking behavior from previously legitimate actors, some of which will cross the line into financial crimes. The UK's Financial Conduct Authority (FCA) has also warned that increases in the cost of living will lead to criminals exploiting people through loan fee fraud and authorized push payment scams. It should be noted that firms also told us they reported more suspicious activity reports (SARs) in 2022 than in 2021. 83 percent said they filed more, a nine percentage point rise on the number who told us they reported more in 2020 than they did in 2019. This indicates that the volume and variety of financial crimes firms reported to law enforcement is rising even before the pressures of an economic downturn bite.

99%

of firms say they're re-evaluating their risk appetite due to the economy.

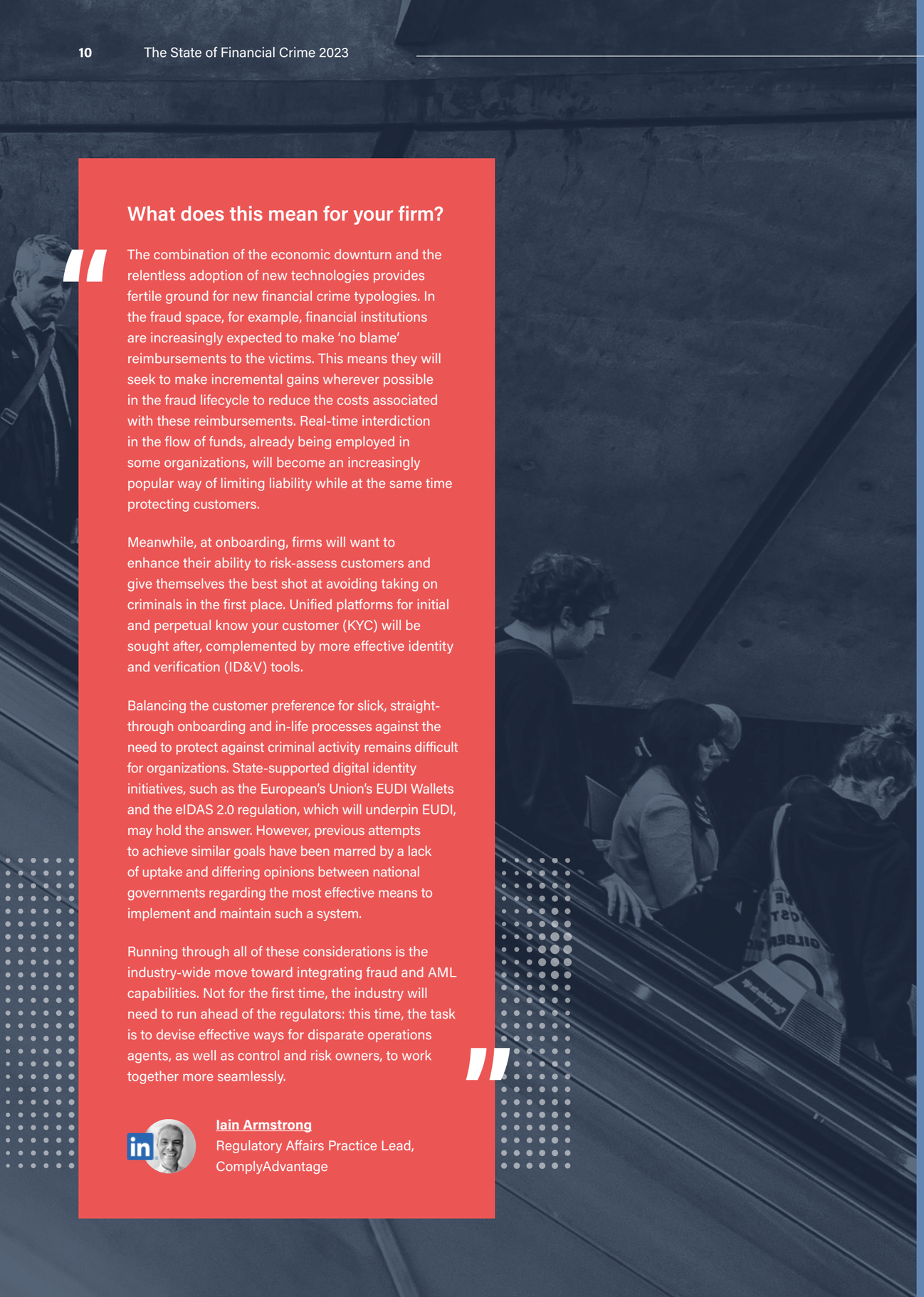
Source: ComplyAdvantage, State of Financial Crime 2023

Of the following, how is your organization's compliance team responding to the uncertain global economic environment?

Source: ComplyAdvantage, State of Financial Crime 2023

While the economic outlook is bleak, compliance professionals are realistic. 59 percent are braced for increased financial crime, with 58 percent planning to hire more staff. Despite expectations that unemployment rates will rise - and double in the US by the end of 2023 - just 11 percent of organizations anticipate reducing the size of their compliance staff.

By contrast, the already-hot employment market for compliance staff is likely to get hotter still. Much of this could be driven by the growth of 'super apps.' Already popularized in Eastern countries thanks to WeChat, Alipay, and others, the rise of similar applications in the West will require firms like Meta, Twitter, and Snapchat that are eying this opportunity to hire fast. While offering greater convenience for consumers, super apps also create spaces where criminals can collude and share information. This could drive a rise in fraud typologies such as account takeovers, payment fraud, and the abuse of referral systems.



What does this mean for your firm?

The combination of the economic downturn and the relentless adoption of new technologies provides fertile ground for new financial crime typologies. In the fraud space, for example, financial institutions are increasingly expected to make 'no blame' reimbursements to the victims. This means they will seek to make incremental gains wherever possible in the fraud lifecycle to reduce the costs associated with these reimbursements. Real-time interdiction in the flow of funds, already being employed in some organizations, will become an increasingly popular way of limiting liability while at the same time protecting customers.

Meanwhile, at onboarding, firms will want to enhance their ability to risk-assess customers and give themselves the best shot at avoiding taking on criminals in the first place. Unified platforms for initial and perpetual know your customer (KYC) will be sought after, complemented by more effective identity and verification (ID&V) tools.

Balancing the customer preference for slick, straight-through onboarding and in-life processes against the need to protect against criminal activity remains difficult for organizations. State-supported digital identity initiatives, such as the European's Union's EUDI Wallets and the eIDAS 2.0 regulation, which will underpin EUDI, may hold the answer. However, previous attempts to achieve similar goals have been marred by a lack of uptake and differing opinions between national governments regarding the most effective means to implement and maintain such a system.

Running through all of these considerations is the industry-wide move toward integrating fraud and AML capabilities. Not for the first time, the industry will need to run ahead of the regulators: this time, the task is to devise effective ways for disparate operations agents, as well as control and risk owners, to work together more seamlessly.

Iain Armstrong
Regulatory Affairs Practice Lead,
ComplyAdvantage

Fraud and scams continue to evolve

Looking ahead to 2023, what types of fraud is your organization most concerned about?

Source: ComplyAdvantage, State of Financial Crime 2023

While concern about fraud overall reached a fever pitch during the pandemic, driven by the exploitation of relief and stimulus schemes, the extent to which criminals leveraged these schemes is still emerging. For example, APT41, a well-known threat actor with ties to the Chinese government, is believed to have stolen tens of millions of dollars in US covid relief benefits. As governments across Europe introduce stimulus payments to offset higher energy bills and the US approves a $430bn green energy subsidy package, 2023 is likely to see a resurgence in concern about government stimulus and subsidies fraud.

Our survey data showed tax and investment fraud as the joint-top concerns for compliance professionals in 2023. While both are likely fuelled by the economic downturn, investment fraud, in particular, often runs counter-cyclically to the economy.

As easier methods of accessing finance dry up, the temptation to resort to bogus schemes offering apparently "market-beating" returns increases. US Sentencing Commission statistics show that while the number of securities and investment fraud offenders has declined over the last five years, the median loss incurred has soared to more than $2,880,000. In August 2022, the Securities and Exchange Commission (SEC) also issued guidance on the growing use of social media platforms to seek investment guidance.

It states that "fraudsters may set up an account name, profile, or handle designed to mimic a particular individual or firm. They may go so far as to create a webpage that uses the real firm's logo, links to the firm's actual website, or references the name of an actual person who works for the firm. Fraudsters may also direct investors to an imposter website by posting comments in the social media accounts of brokers, investment advisers, or other sources of market information."

Credit and debit card fraud remained a major concern, cited by 39 percent of respondents. Much of this is driven by e-commerce, with purchases made via phone, internet, or mail-order using stolen cards estimated to surpass $10bn by 2024. The popularity of credit cards for online purchases means they are involved in a significant amount of this fraud.

Emerging typologies such as synthetic identity fraud also featured significantly, surpassing concern about crimes such as elder and romance fraud. KPMG cites synthetic ID fraud as the fastest-growing financial crime in the United States, costing banks more than $6bn. 2023 is likely to see synthetic ID fraud grow further, with criminals identifying new ways to exploit consumers aligned with ongoing economic pressures. One example of this is mortgage fraud. As rising interest rates push up mortgage costs in many countries, those desperate to attain financing may seek to use more advanced but increasingly accessible technologies to bypass increasingly stringent lender requirements.

2023 is also likely to be the year when more firms leap into the metaverse. As a result, so too will more criminals. It's estimated one in four people will spend at least an hour a day in the Metaverse by 2026. The World Economic Forum, in partnership with INTERPOL, Meta, Microsoft, and others, have warned that social engineering scams, extremism, and misinformation are likely to be early challenges. Recognizing that the Metaverse is "already here," INTERPOL has also launched its own metaverse, giving users a tour of its headquarters and enabling them to interact with other officers and take training courses. With analysts forecasting a virtual economy in the metaverse enabled by virtual currencies and non-fungible tokens (NFTs), the financial crime risks associated with crypto are also likely to collide with new virtual realities. According to Morgan Stanley, risks include NFT price manipulations and counterfeit and malicious NFTs.

Compounding these fraud challenges is the continued rise of e-commerce, with global sales expected to rise fifty-six percent by 2026, reaching $8.1 trillion. As e-commerce volumes rise, so will fraudsters' desire to exploit weaknesses in these platforms. Seasonal surges in demand also create uneven pressures throughout the year, with spikes occurring, for example, over Thanksgiving and Christmas.

Debates around enforcement effectiveness and liability will also persist through 2023. In the UK, fraud represents 40 percent of reported crime, but just 2 percent of police funding is dedicated to combating it. In Singapore, police figures revealed the Anti-Scam Centre froze over 7,800 bank accounts, recovering almost $80m in the first half of 2022. However, that accounted for just 31 percent of the amount consumers lost to scams. There's some evidence that low confidence in law enforcement's ability to tackle fraud is also affecting consumers' willingness to report it. In Australia, a government survey showed just half of those who experienced a scam reported it.

Meanwhile, in the UK, the government has pledged to give the Payment Systems Regulator the power to force firms to reimburse victims in certain cases, such as authorized push payment scams. In many jurisdictions, such as the US, regulations still stipulate that if consumers authorize the transfer, the financial institution cannot be held liable, and the customer can receive a refund.

However, in 2022 the Consumer Financial Protection Bureau issued new guidance that if an account holder shares their credentials with a third party that is compromised and a fraudster accesses the consumer's account to move money, then the bank is responsible. Industry figures recognize the importance of retaining customer trust but are also concerned about the impact of new guidance on emerging use cases such as open banking.

What does this mean for your firm?

"Financial crimes and cybercrime are invariably linked. For every dollar of fraud, institutions lose nearly three dollars once associated costs are added to the fraud loss itself. In a world where customers interact mostly through digital channels, this can quickly become costly for organizations. As a significant amount of financial fraud takes place through digital technologies, cybercriminals are recruited by fraudsters to exploit emerging payment technologies to launder their illicit gains whilst taking advantage of the vulnerabilities inherent to real time payments, automation and digitization. With the number of Metaverse users growing and the technology further developing, it is important for law enforcement bodies to experience the Metaverse for themselves. Fully operational, the INTERPOL Metaverse allows registered users to tour a virtual copy of the INTERPOL General Secretariat headquarters in Lyon, France without any geographical or physical boundaries, and interact with other officers via their avatars."

Alia Mahmud
Regulatory Affairs Practice Lead, ComplyAdvantage

Ransomware activities diversify

Ransomware has continued to increase in scale and variety. An analysis published by the Financial Crimes Enforcement Network (FinCEN) showed that, compared to 2020, reported ransomware incidents in the second half of 2021 increased by more than 50 percent. Ransomware-related BSA filings in 2021 hit $1.2 billion. Much of this was driven by Russia-related ransomware variants, a trend likely to accelerate as Russia continues its aggressive cyberwarfare around the war in Ukraine.

2022 also saw an acceleration in the convergence of ransomware and cryptocurrencies, most notably through Deadbolt, a group attacking network-attached storage (NAS) devices and vendors. Once the ransom payment is made in Bitcoin, the decryption key is sent automatically. Deadbolt infections soared by 674 percent between June and September 2022 alone, with most infections found in the US, Germany, and Italy.

Regulators have taken action to inform and advise firms in their jurisdictions about how they can best tackle ransomware risks. In April 2022, the Australian Transaction Reports and Analysis Centre (AUSTRAC) issued a report highlighting several financial indicators of ransomware, including rapid increases in customers' account limits and encountering a photograph of data on a computer screen as part of the customer verification process at onboarding.

The International Counter Ransomware Initiative (CRI) also hosted its second summit in late 2022, focused on large-scale cyber attacks and money laundering via digital currencies. Through 2023, it will focus on establishing a ransomware taskforce, instituting active private sector engagement, and coordinating priority targets through a single framework.

Alongside Russia, state-sponsored ransomware actors in North Korea and Iran have become more critical and will remain so. In April, the US Office of Foreign Asset Control (OFAC) expanded its sanctions regime covering alleged North Korean wallets following the hack of blockchain game Axie Infinity's Ronin bridge, which saw $600m in cryptocurrency stolen. In September 2022, three Iranian nationals were charged with orchestrating a scheme to hack multiple US computer networks, including government agencies, nonprofits, and healthcare facilities.

It's unclear exactly how the ongoing volatility in the cryptocurrency market will affect ransomware actors' preference for crypto as a payment method. Some analysts have argued the unique characteristics of crypto make it irreplaceable as a payment method. Others have highlighted that devaluations will force criminals into more frequent - and aggressive - attacks to sustain their way of life.

What does this mean for your firm?

"Firms need to keep their cyber defenses, data hygiene, and training programs under continuous review so they're able to rapidly adapt to the shifting ransomware landscape as effectively as possible. Familiarity with the latest behaviors, and any specific forms of ransomware targeting their sector, will be critical. It's also critical to review the latest guidance from regulators in relevant jurisdictions, as they will continue to issue practical information on the risks firms face and any actions they should take. Digital-native firms not yet operating Bug Bounty programs would do well to consider implementing them, alongside regularly-scheduled pen testing exercises"

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

Drug trafficking destabilizes South America

Throughout 2022 further evidence emerged of the vast, growing scale of cocaine production across Latin America and its import routes into the US, Europe, and Asia Pacific. The UN Office on Drugs and Crime (UNODC) issued data showing global production soared to 1,982 tonnes in 2020 - an 11 percent rise on 2019 and almost double 2014 levels. Growing production has also seen drug cartels expand their reach across the region, with Paraguay, Uruguay, and Chile all experiencing higher drug-related violence in 2022. Antwerp's port officials seized more cocaine than any other major European port in 2021. They noted the three main sources of shipments to be Ecuador, Paraguay, and Panama - none of which are major drug producers. The UNODC now believes all but three of Latin America's 21 mainland countries are "main countries of course or transit" for cocaine. The growing power and reach of drug cartels - and the threat to the stability of regional states this poses - has been reflected in enforcement actions issued in 2022.

One clear focus is on those who "enable" cartel activity. In July 2022, OFAC sanctioned an individual it said was trafficking high-caliber firearms to CJNG, one of Mexico's top cartels. In October, an attorney who laundered drug money for the Sinaloa Cartel was sentenced to more than 15 years in a US prison.

The acceleration of cocaine production has collided with the sustained - and rising - challenge of synthetic and opiate drug use in the US and Canada in particular. In November 2022, the Financial Action Task Force (FATF) issued its inaugural report on money laundering from fentanyl and synthetic opioids. With at least 82 percent of opioid-induced overdoses involving synthetic opioids, the Biden administration has indicated it intends to pursue a "whole-of-government" response.

As the pandemic recedes and cash-driven nightlife venues around the world return, these pressures will only intensify. Through 2022, regulators and law enforcement in countries including the US and Australia have focused on the AML risks associated with cash-intensive businesses. AUSTRAC launched a national education campaign for pubs and clubs, visiting more than 200 venues. It also began enforcement proceedings against multiple venues.

What does this mean for your firm?

"Firms need to fully assess and understand their exposure not just to drug trafficking itself but related typologies that could indicate drug-related activities. The FATF's report highlights behaviors including money laundering through cash-intensive businesses, trade-based money laundering, and wire transfers, especially between front and shell companies. It also argues that better information sharing, investigator training, and awareness of the risks related to new technologies like dark web marketplaces are critical. Retail financial services firms should be mindful that increased trafficking ultimately filters down to the level of everyday life. Trafficking eventually translates to street-level crime such as money muling, or the 'county lines' activities seen in the UK, even in jurisdictions far removed from the countries where illegal drugs originate."

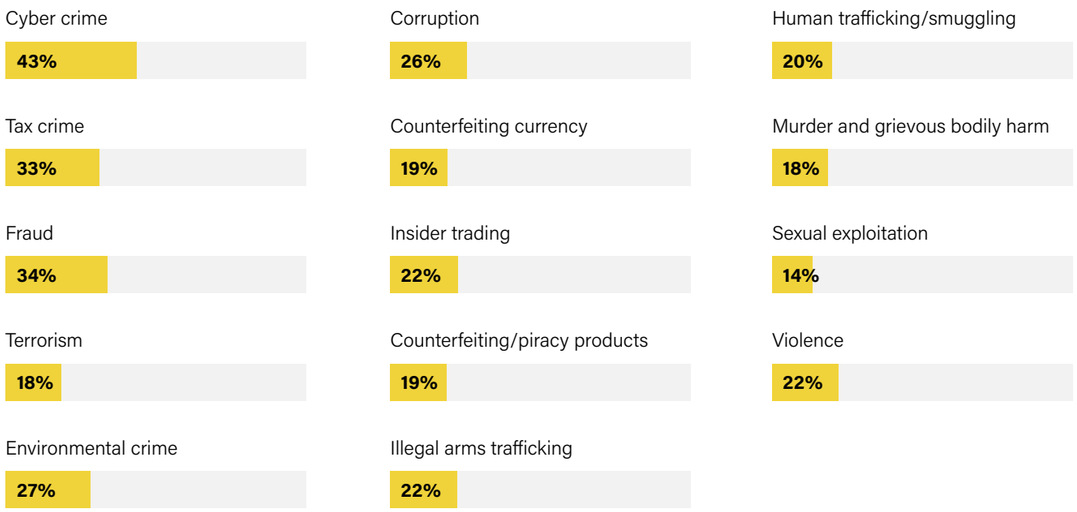
Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

Environmental crime surges as enforcement lags

International concern about environmental crimes and wildlife trafficking soared in 2022, reflecting the threat posed to food security, political stability, conflict, and forced migration. When asked which predicate offenses were most important to their organizations, more than one in four selected environmental crime, making it one of the top selected offenses. This is despite its inclusion in our survey for the first time in 2022. Environmental crime was also the second highest typology of concern for firms when submitting suspicious activity reports (SARs), behind only tax evasion.

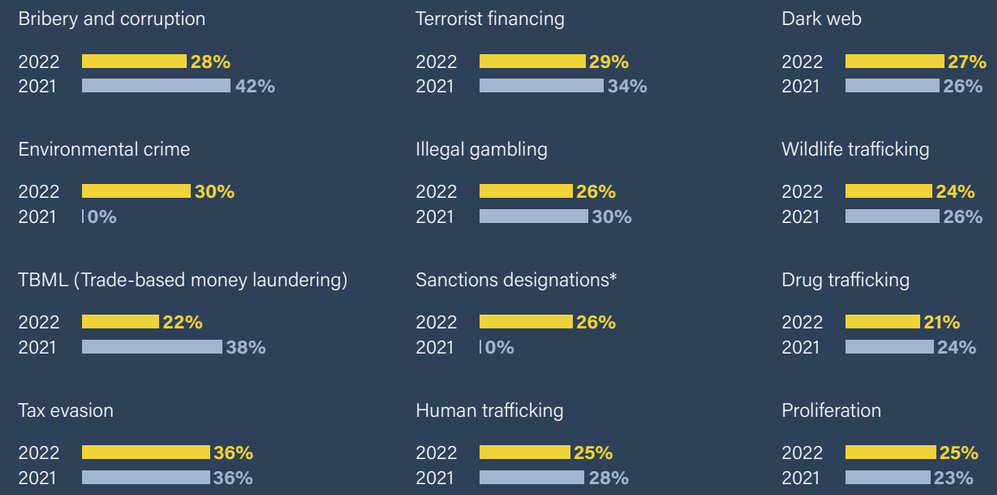
The global picture mirrors compliance officers' concerns. Think tank Chatham House found that 15 percent of all timber exports from 37 exporting countries were illegal, with the majority coming from China, Brazil, Indonesia, and Russia. Wildlife crimes have also surged, with South Africa experiencing record levels of poaching to meet high demand from Asia. In October 2022, a month-long World Customs Organization (WCO) law enforcement operation to enforce CITES and disrupt wildlife crime covered 125 countries. It led to the identification of 141 companies suspected of engaging in illegal sales, alongside over 2,200 seizures, and the launch of numerous investigations.

What predicate offenses are most important for your organization to screen against?



Source: ComplyAdvantage, State of Financial Crime 2023

When submitting suspicious activity reports, what typology/ies is your organization most concerned with?



*This category was added for the first time in 2022

Source: ComplyAdvantage, State of Financial Crime 2023

An increasing range of online channels, such as e-commerce sites, social media, and offshore commerce, are also being used to fuel wildlife cyber-crimes and sell goods outside the CITES regulatory framework. For example, research from WWF, a leading conservation organization, showed the online illegal wildlife trade in Myanmar increased by 74 percent from 2020 to 2021. Virtual private networks (VPNs), proxy servers, the Onion Router (TOR), the darknet, mobile payments providers, cryptocurrency, TikTok videos, and end-to-end encrypted apps are all being exploited to sell illicit goods and protect the privacy and anonymity of criminals. The Coalition to End Wildlife Trafficking Online identified that internet companies blocked or removed over 11.6 million posts and listings of illegal wildlife for sale. They further received reports of over 11,000 listings for illegal wildlife via the Coalition's citizen science Cyber Spotter program. This trend is likely to continue.

Some of the growth in demand driving environmental and wildlife crimes can be attributed to the easing of pandemic restrictions, which has made activities like poaching easier. In June 2022, China also suspended a wildlife trade ban introduced in January 2020 to tackle potential sources of COVID spread. The global downturn has already led to scaled-based resources, resulting in less capacity to train rangers and investigators in source countries, including Botswana, South Africa, Kenya, Namibia, and Tanzania. Against this backdrop, United for Wildlife estimates illegal wildlife traders will "return to full profitability within 2-3 years."

Policymakers and regulators globally are taking note. In November 2022, the European Commission adopted a revised EU Action Plan to end the illegal wildlife trade. Its goals include tackling the root causes of wildlife trafficking, strengthening legal frameworks, more effective regulatory enforcement, and improving partnerships. Singapore's parliament also discussed the issue in April 2022, with the government highlighting the "more sophisticated" behavior of criminals and the growing importance of "close collaboration between the government and private sector." In the US, in October 2022, OFAC sanctioned a number of Malaysian nationals, and the Sunrise Greenland Sdn. Bhd. for the "cruel trafficking of endangered and threatened wildlife and the products of brutal poaching." This involved transporting rhino horns, ivory, and pangolins from Africa through Malaysia and Laos, ultimately ending up in Vietnam and China.

What does this mean for your firm?

Firms should ensure that they have anti-money laundering controls in place that are capable of identifying and mitigating the risk of environmental crimes. They should also assess their residual risk exposure through frequent enterprise-wide risk assessments. With new and emerging environmental financial crime typologies, firms should provide adequate training that includes risk indicators and typologies for illegal wildlife, waste trafficking, and other environmental crimes. Firms need to embed controls that are sophisticated enough to identify and mitigate these risks. This includes enhancing their transaction monitoring scenarios and rules to identify suspicious transactions and behavior that could lead to customers and payment methods that are being used to perpetrate environmental crimes.

We also anticipate that in 2023 more firms will become wise to the way environmental crime intersects with other types of financial crime. For example, successful investigations into wildlife crimes invariably reveal that those crimes were facilitated by bribery and corruption (e.g., government or port officials), fraud (e.g., Customs & Excise documentation), and money laundering (e.g., the dispersal of profits). An increasing awareness of this intersectionality will put firms in a better position to understand, prioritize and control against risks associated with environmental crime.

Alia Mahmud
Regulatory Affairs Practice Lead, ComplyAdvantage

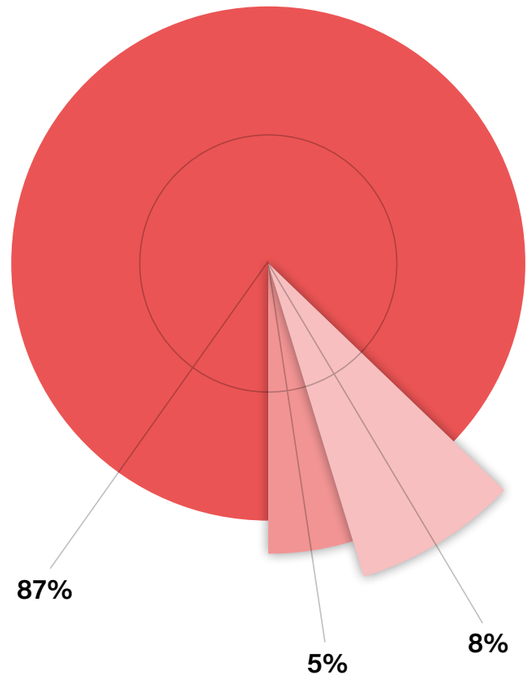
Crowdfunding is fueling political extremism

Protests across Ottawa and US-Canada border crossings have elevated global concern about the use of crowdfunding platforms for extremist groups. On February 4th, 2022, GoFundMe closed a campaign supporting the "Freedom Convoy" due to concern it had become an "occupation" and amidst widespread reports of violence. The group then pivoted to GiveSendGo, a platform which, according to The Washington Post, describes itself as "the leader in Christian fundraising," where it raised over $9m.

This year our global survey asked about the use of decentralized finance platforms to support extremist political groups for the first time. 87 percent of respondents said they'd seen an increase in the use of these platforms to fund extremism, with 31 percent believing the growth to be "significant." Crowdfunding has also supported Islamic State (IS) operatives in Syria. Reporting indicates family members of young men trapped in Syrian camps have attempted to use the Telegram messenger service to "bring them to safety."

It's believed some of those looking to escape are doing so to fight for IS. In a report issued on March 1, 2022, the US Treasury explained how domestic extremists have used legal fundraising methods to support their activities, making them harder to detect. The Treasury also highlighted the pandemic's role in making these platforms "a necessity rather than a convenience."

Over the last 12 months, what change, if any, have you seen in attempts to use decentralized finance platforms (e.g. crowdfunding) to fund extremist political groups?



Source: ComplyAdvantage, State of Financial Crime 2023

What does this mean for your firm?

It's clear that many crowdfunding platforms have been caught short by the surging demand for their services. Crowdfunding, in conjunction with cryptocurrencies and social media, increases the risks of terrorist financing by allowing bad actors to utilize the reach of crowdfunding platforms and crypto asset technologies to gain support from followers and receive funds. Compliance officers working for firms offering decentralized finance services must be aware of the emerging regulations in the cryptocurrency and crowdfunding space to ensure they have adequate, effective, scalable financial crime control solutions in place. This will include transaction monitoring rules tailored to the unique typologies and behaviors they should screen for. Crowdfunding platform providers should familiarize themselves with the new EU regulation for crowdfunding service providers. Banks and other providers working with crowdfunding organizations should perform enhanced due diligence before agreeing to a partnership, or they risk being exposed to financial crime risks and the bad publicity that comes with these.

Alia Mahmud
Regulatory Affairs Practice Lead,
ComplyAdvantage

← Previous section

Next section →

Sanctions & Geopolitics

2022 was a year defined and shaped by sanctions on an unprecedented scale. This section looks at the prospects for Russia and Ukraine in the year ahead, simmering US-China tensions, and why we should expect the return of familiar hotspots including Iran and North Korea.

The full-scale Russian invasion of Ukraine began in February 2022 and accelerated pre-existing trends in economic statecraft, with a coalition of democratic countries imposing massive coordinated sanctions against the Putin regime. This Ukrainian 'playbook' on sanctions could be used again in the event of similar crises in the future.

At the close of 2021, we expected the geopolitics of 2022 to be dominated by friction between increasingly polarized camps of authoritarian regimes and a coalition of western-democratic countries (primarily the US, Canada, EU, UK, Japan, Australia, and several other European and Asia-Pacific jurisdictions), with economic statecraft playing a major role in the West's approach to the contest.

Shockingly, our assessment was proven correct by the full Russian invasion of Ukraine on February 24. The invasion was met by the most comprehensive sanctions imposed against a major power since the end of the Second World War, with the US, European Union (EU), and others coordinating their actions in unprecedented ways. 2023 begins with the war ongoing and no sign of an immediate resolution. Western sanctions against Russia are thus likely to remain and tighten further in 2023. However, their loosening will play an important role in ending the war if Putin decides he cannot achieve his goals militarily.

At the same time, tensions have remained high between western countries and perennial international troublemakers Iran and North Korea. The revival of the Iran nuclear deal now looks unlikely, and Pyongyang has caused consternation with numerous missile tests. Further tensions and new weapons proliferation-related sanctions seem likely in 2023, but these will not come from the UN Security Council (UNSC) as before, with Russia and China acting as a block on action initiated by the US, France, and the UK, the Council's permanent western members. Any further measures on weapons proliferation in 2023 will likely come from the US and its allies alone.

The final headline challenge is China, on which western countries have imposed a range of sanctions for human rights abuses and domestic repression. In comparison to recent years, 2022 has been relatively quiet, although the US has kept up the pressure on the Chinese technology sector. There was also a brief flare-up in August over the status of Taiwan between the US and China, which, while in effect self-governing, is seen as a part of China by Beijing. Although neither the US nor China is likely to stimulate a further crisis in 2023, one cannot be ruled out, with any Chinese attempt to intimidate Taiwan through military means leading to a similar western sanctions response to that seen against Russia.

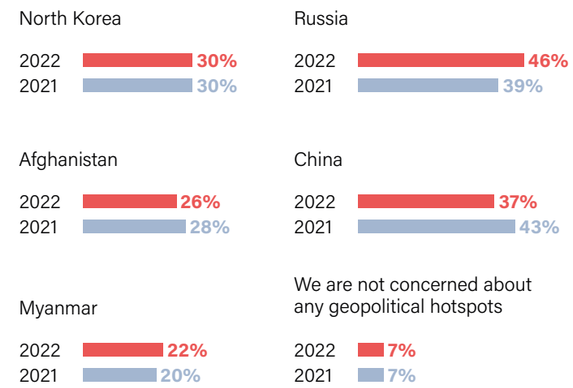
What are Sanctions?

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. Nearly all countries follow the sanctions imposed by the UNSC, but an increasing number have their autonomous regimes, of which the US is the most influential. Sanctions commonly target entities such as official institutions, businesses, groups, and networks, as well as individuals. When imposing sanctions, sanctioning bodies commonly prohibit those under their authority from undertaking economic and financial interactions with the target or freeze the target's accessible assets. Individual sanctions also now commonly involve travel bans to areas under the sanctioning body's control or via carriers under its authority. For more details, see our report 'The Evolving World of Sanctions'

Major Hotspots: Russia

In our State of Financial Crime Report 2022 report, we expected China to be the primary maker of geopolitical waves. But as we now know, the Russian invasion of Ukraine has been the dominating factor in international politics during the year. But Russian bellicosity towards Ukraine was rising, and our prediction - that "if Russia escalates the situation further, the use of coordinated sanctions is highly likely," has proven an accurate reflection of the western democratic coalition's response. Unsurprisingly, as a result of the war, Russia topped this year's list of geopolitical hotspots firms are most concerned about.

Which of the following geopolitical hotspots is your organization most concerned about?



Source: ComplyAdvantage, State of Financial Crime 2023

Contours of the Crisis

Russia, the US, and its allies have been taking increasingly confrontational stances toward each other over the last decade. On one side, President Vladimir Putin has claimed that western powers have sought to encircle Russia and undermine him. On the other, the democratic world has criticized Putin for what it sees as a flagrant disregard of international standards in his regime's treatment of domestic dissidents such as Alexei Navalny, attacks on dissidents living overseas, interference in western politics and military adventurism.

But the most intractable area of disagreement has been over Russia's neighbor Ukraine. Putin sees the country as part of Russia's sphere of influence and, therefore, not a suitable member of either the EU or NATO, organizations Ukraine has repeatedly expressed an interest in joining. Tensions between Russia and western countries over Ukraine have flared several times over the last decade following Russia's illegal annexation of the Ukrainian region of Crimea in March 2014 and its support of an ongoing proxy war against the Ukrainian government in eastern Ukraine. At the end of 2021, tensions rose again, with Putin re-stating his concerns about Ukraine's increasingly pro-western orientation and increasing military forces on the Ukrainian border. Despite the assessments of most western observers that Russia would not take extreme action, Putin recognized the independence of the rebel-controlled areas in Donetsk and Luhansk on February 21, 2022. Days later, on February 24, 2022, he launched a full-scale conventional invasion of Ukraine, described as a 'special military operation.'

The Western Response

Before the invasion in February, western countries had varied sanctions in place against Russia in response to a range of issues, including its abuse of human rights, regime corruption, overseas assassinations, overseas political interference, cyber-attacks, and military aggression. The US had the most extensive of the existing national regimes, targeting oligarchs closely linked to President Putin, political and military leaders, Russian military and energy sectors, and those directly involved in perpetrating abuses and corruption against dissidents and whistle-blowers such as the Russian accountant, Sergei Magnitsky. Magnitsky died in Russian custody in November 2009 after revealing a massive fraud by officials (see box on 'US Sanctions'). The EU, Canada, the UK, and others had followed the US lead in several of these areas in recent years, but at the start of 2022, they still had much more limited regimes directed against Russian activities.

But the invasion changed this situation dramatically. The US imposed further measures, joined by a wide spectrum of others, most notably the EU, representing 27 European countries, as well as Norway, Switzerland, Iceland, the UK, Canada, Australia, and New Zealand (four of the so-called 'Five Eyes' intelligence alliance). In the Asia-Pacific Region, they were joined by Japan, South Korea, Singapore, and Taiwan. In some of these cases - the imposition of autonomous national sanctions outside of the UN framework - Switzerland, for example - has happened for the first time. Although the most substantial sanctions were imposed in the first few months after the invasion, new packages have been introduced across the year as the invasion has continued; as of the time of writing, the EU had formalized its eighth round of restrictive measures.

The countries have not imposed identical measures, but their responses have shown unprecedented levels of coordination and commonality. Viewed thematically, the key target areas for democratic countries have comprised:

- **Individual 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 key institutions within Russia's financial sector, including the Central Bank of Russia, its National Wealth Fund, and the Ministry of Finance. These are designed to prevent the Russian government from using foreign currency reserves or selling assets such as gold to fund the war. Several major Russian financial institutions, including its largest commercial bank, Sberbank, have been removed from the SWIFT messaging system, which supports international financial transactions. The crypto asset sector has also been affected, with the US designating Crypto Assets Services Providers (CASPs) and individual wallets used in suspected sanctions evasion and fundraising across the year.

The EU placed a 10,000 Euro threshold for cross-border cryptocurrency transactions with Russian individuals and entities outside the EU in April 2022, later becoming a full ban in October.

In addition, Singapore warned its CASP sector in October to ensure it complied with Russian designations, especially where individuals appeared to be seeking to raise funds to support the Russian war effort through cryptocurrency.

- **Sectoral Sanctions:** These have included a variety of export and/or import controls on strategic Russian industries and firms involved in the production or procurement of weapons, dual-use goods (e.g., drones and drone software), advanced technology (e.g., quantum computers and advanced semiconductors), iron and steel, logistics and transport, and - most controversially - the energy sector. On March 8, US President Joe Biden prohibited the import of all Russian oil, gas, Liquid Natural Gas (LNG), and coal into the US. The EU and UK have also taken a range of measures to phase out the import of Russian oil, refined oil products, and coal, but European controls on Russian natural gas have been partial and mixed, reflecting the EU's dependency on Russia for around 40 percent of its annual natural gas requirement. Some measures have been taken, with Germany suspending the opening of the Nord Stream 2 gas pipeline between Russia and Germany indefinitely. Still, a ban on gas has not emerged, with the EU only making a rhetorical commitment to eliminating reliance on Russian fossil fuels, including gas, by 2027. One area of innovation in sectoral packages included US and UK sanctions in May, and the EU in June, on the provision of corporate and professional services exports to individuals in Russia, reflecting increasing concerns amongst regulators and law enforcement about the roles played by professional enablers in financial crime.

Alongside these measures, the sanctioning countries have also created mechanisms for more effective sanction implementation. A Russian Elites, Proxies, and Oligarchs (REPO) Task Force was announced in concept by the leaders of the G7 countries and the EU on February 26 (subsequently joined by Australia), with the intention of "identifying and freezing the assets of sanctioned individuals and companies" through information-sharing and joint-working. This international effort was supported by the subsequent creation of national teams, such as the US's Task Force KleptoCapture by the US Department of Justice (DoJ), and the UK's Combating Kleptocracy Cell, based in the National Crime Agency (NCA).

As part of its remit, the REPO Task Force has also fostered discussions on how frozen Russian assets could be seized by sanctioning authorities (the so-called move 'From Freeze to Seize'), and used to help rebuild Ukraine, a major legal challenge because seizure and forfeiture of an individual or entity's asset are commonly triggered by domestic criminal activity, rather than a regime's breach of international law.

So far, the US has sought to initiate cases using pragmatic precedents based on existing fraud, money laundering, and sanctions legislation - see, for example, the US requested the seizure of oligarch Viktor Vekselberg's yacht in Spain in April 2022 on these grounds. But it is looking to provide surer legal footing in the future by adding sanctions evasion to the Racketeer Influenced and Corrupt Organizations (RICO) Act, most commonly used as a basis for seizure in racketeering and organized crime cases. The European Commission's proposed Directive of Asset Recovery and Confiscation, published in May 2022, also proposes to make sanctions evasion an offense that can be used as the justification for asset recovery. In contrast, the Canadian government is proposing to use a previously unpassed piece of legislation, the Frozen Assets Repurposing Act, which would allow the seizure of assets from individuals designated as risks to the "grave breach of international security."

The Canadian government is proposing to use a previously unpassed piece of legislation, the Frozen Assets Repurposing Act, which would allow the seizure of assets from individuals designated as risks to the "grave breach of international security."

Retaliatory Russian Sanctions

Russian rhetoric in response to western sanctions has been fierce. In March, President Putin described them as a form of "economic war." However, Russia's own counter-sanctions have been much less sweeping. Russia has placed targeted sanctions on leading US and other western politicians, but announcements have specified travel bans without financial measures. More broadly, Russia has placed several controls on foreign currency transactions and debt repayments by foreign businesses and has designated sanctioning countries as 'unfriendly,' restricting commercial access to Russia for companies from those jurisdictions without specific approval.

The Putin regime has also used Europe's dependency on gas as a weapon against it, albeit in a calibrated fashion that has not fully cut off supply - a move that would massively undermine Russia's own earning of valuable foreign hard currency. In September, Russia indefinitely closed the Nord Stream 1 pipeline under the Baltic Sea, saying that the pipeline was damaged. In reply, the EU stated that the pipeline was damaged - due to Russian sabotage. In September 2022, Dmitry Peskov, the senior spokesman for Putin, said the pipeline would not be re-opened until the "collective west" had removed its sanctions.

Russia has also sought to find ways to use energy to poke holes in western sanctions, primarily through revising payment methods. In March 2022, President Putin announced that buyers would need to pay for gas in a scheme requiring initial payment in an international currency such as the Euro or the US dollar, followed by its conversion into rouble. However, this risked European buyers breaching sanctions because of the role that would need to be played in converting currencies by Russia's Central Bank - itself designated by the EU. This has led the EU to largely bow to Russian demands while recommending buyers issue statements to indicate that they deem the initial payments in international currency the completion of the transaction as a form of legal cover.

A further area of Russian economic countermeasures has been its intermittent blockade of Ukrainian wheat, corn, and other cereal exports from Ukraine's Black Sea ports. From the spring through until summer, Russian naval activities made it impossible for Ukraine - one of the world's leading cereal producers - to export its goods, driving up food prices globally. In July, Russia agreed to allow exports to resume under a deal brokered by Turkey, but in October, it withdrew from the arrangement briefly in response to Ukrainian drone attacks on Russian ships. Although the deal remained in place at year-end, Russia has re-stated its right to withdraw, opening up the possibility of further global food security issues in the future.

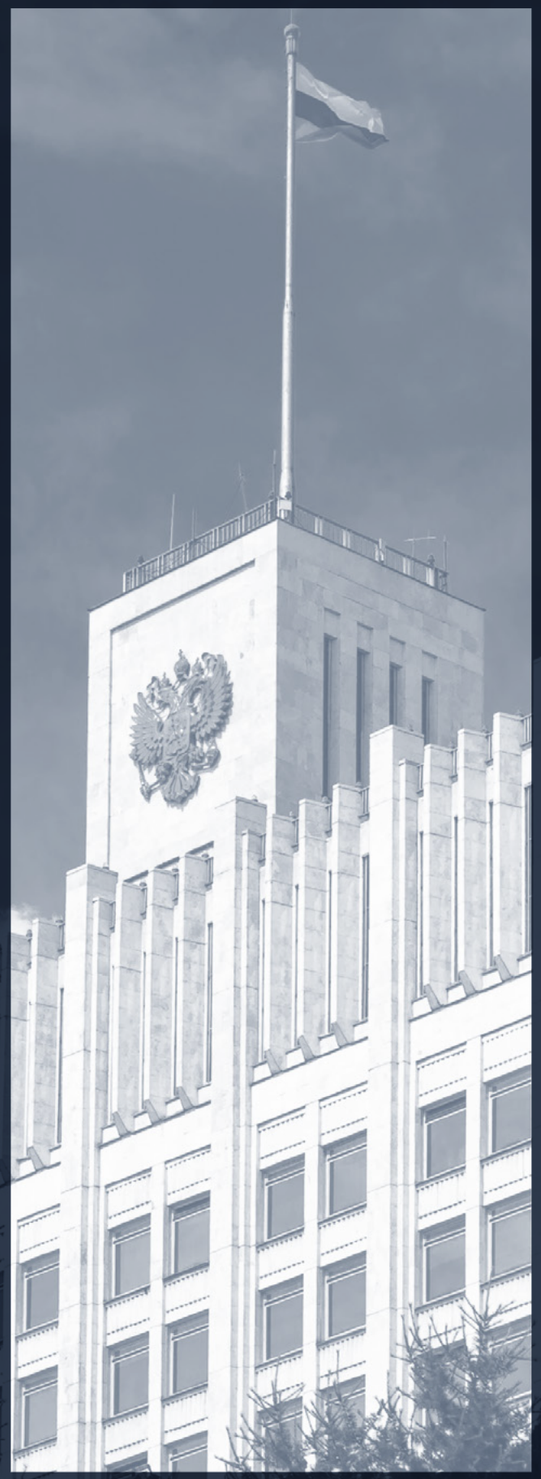
The Effectiveness of Sanctions on Russia

How effective have western sanctions on Russia been? Certainly, the Russian economy as a whole is undergoing a severe contraction that is likely to continue through 2023. The performance of the Russian military also appears to have been undermined by sanctions which have limited its ability to resupply. But despite these undeniable effects, sanctions have not so far succeeded in their main aim: convincing President Putin to withdraw in full from Ukraine. Precisely why is unknowable, but Putin's past behavior suggests that he has a high threshold for economic pain and is willing to accept difficulties as long as they do not cause levels of political unrest which might imperil his own position. In addition, it is also clear that sanctions are not as effective as they might be, probably reflecting a range of vulnerabilities in western sanctions regimes:

- **Critical Gaps in Sector Coverage:** The most obvious gap is the absence of an EU ban on the import of Russian natural gas, which continues to generate large revenues for Russia's largest gas company, the state-run giant Gazprom. According to an analysis mid-year by the Independent Commodity Intelligence Services, Gazprom was making as much per day (around $105 million) from gas exports to Europe as it had been the year before.

- **Exemptions and Phased Introductions:** Within the EU, several member states have been awarded exemptions on sanctions where they are highly dependent on a commercial relationship with Russia. For example, Bulgaria has an exemption from oil sanctions until 2024 due to its reliance on a Russian pipeline and a single domestic oil refinery owned by the Russian company Lukoil. Many sanctions have had significant lead-in time, allowing Russian individuals and companies to take action to change ownership structures or fully divest.

- **The Role of Neutral Countries:** The level of international partnership on Russian sanctions has been unprecedented. However, most countries do not have their own autonomous regimes, indicating - as has India - that it will only follow UNSC measures, thus providing alternative markets for Russia. As a result, Russia's oil exports have been largely re-directed from Europe to other markets in Asia, including major economies such as China and India, underpinned by major discounts averaging $30 dollars on a barrel of crude oil. Jurisdictions such as UAE have also become new safe havens for Russian oligarchs seeking to protect their assets.



In addition, there has been ample evidence of Russian individuals, businesses, and other entities demonstrating a sophisticated capacity to exploit gaps and weaknesses in western sanctions:

- **Procuring Goods Through Proxies:** Following long practice, the Russian military and intelligence services have continued to procure dual-use and technology using fronts and proxies in a number of countries. In March, the US Treasury's Office for Foreign Asset Control (OFAC), its sanctions administrator, announced designations related to one such network centered on the Moscow-based Serniya Engineering, which involved clandestine procurement through companies in numerous countries, including Spain, the UK, and Singapore. In October, OFAC identified and designated a further network led by Yury Orekhov, a Russian national, and linked businesses based in Germany and the UAE.

- **Obfuscating Russian Origins of Banned Commodities:** Russia has, in part, been able to evade commodities bans by using well-worn methods perfected by long-term sanctions targets such as Iran and North Korea. To hide oil sales, Russia has re-registered oil tankers to 'flags of convenience' such as St Kitts and Nevis and Liberia, blended its own oil with other nations' supplies, and used ship-to-ship transfers at sea with transponders turned off to hide the Russian origin of the commodity. There are also indications that Russia is exploiting neutral countries as conduits for 'origin laundering' commodities. Gold exports from the UAE to Switzerland - the main location of the world's gold refinement industry - rose to 36 tonnes in the month following the invasion, more in one month than in any month of the previous six years. This has led to a suspicion in the industry that Russia was using UAE's neutrality as a way to continue engagement in the gold trade.

- **Changing Ownership and Corporate Structures**: Past sanctions experience has provided oligarchs and businesses with a ready playbook for pre-empting potential sanctions with changes of ownership. The International Consortium of Investigative Journalists (ICIJ) has revealed, for example, that in the wake of the invasion, oligarch Alexei Mordashov, one of Russia's richest men, quickly transferred his shares in the German travel group TUI to a Caribbean shell company that his personal partner actually owned.

- U**sing Cryptocurrency:** As we predicted at the start of the war, Russian citizens, in general, have shown a willingness to turn to crypto assets - especially stablecoins - as a store of value and means of exchange in 2022. In the case of those specifically targeted by sanctions, there have been indications that they, too, have also looked to crypto as one avenue to work around western measures, with Russian oligarchs using cryptocurrency to move assets and pay for goods in locations such as the UAE. In July, the UK's Joint Money Laundering Intelligence Taskforce (JMLIT), a public-private partnership, issued an alert warning that designated individuals were exploring using cryptocurrencies to evade sanctions. Nonetheless, although cryptocurrencies appear to be of increasing interest to the Russian population at large, and a valuable tool for the Russian elite, assessments by crypto analytic firms such as Chainalysis and US officials have indicated that the cryptocurrency market lacks sufficient liquidity to support the evasion of sanctions at a national scale.

- **Using Western Legal Systems:** Following precedents such as Roman Abramovich's 2021 libel case against Catherine Belton's book on Putin and his associates, 'Putin's People,' Russian oligarchs have used western legal systems to fight back against designation. Yevgeny Prigozhin, a billionaire caterer, known as 'Putin's Chef' has allegedly engaged US and UK law firms to challenge his designation, while Alexander Abramov, a Russian steel mogul, has launched legal action in Australia against the minister for foreign affairs for his designation. According to Bloomberg, in July 2022, 30 individuals had also taken the EU to court seeking their removal from the Russian sanctions lists.

Prospects for 2023

The development of sanctions against Russia in 2023 is likely to hinge on developments on the battlefield in Ukraine itself. So far, the Russians have been unable to either topple the Ukrainian government of President Volodymyr Zelenskyy or occupy the country. Moreover, although the Russian military has made territorial gains in the east and south of Ukraine, illegally annexing the Ukrainian regions of Donetsk, Luhansk, Kherson, and Zaporizhzhia on September 30, 2022, Ukrainian forces made several successful counter-offensives. In early November, Russian soldiers were forced to evacuate the city of Kherson in the face of Ukrainian attacks, despite its supposed annexation. At year-end, fighting continued across the east and south of the country, with Russia facing gradual losses of previously gained territory. Its response so far has been to mount drone attacks on energy infrastructure and civilians in the rest of Ukraine, seeking to undermine Ukrainian morale.

It is feasible that Russia will achieve a conventional breakthrough in 2023, possibly helped by a Belarusian entry into the war on Russia's side or by an influx of new recruits to the Russian army following a decision to mobilize in full, both of which were discussed in 2022 but did not occur. Despite much speculation about full mobilization, Putin decided on only a partial call-up of reservists in September, possibly fearing political discontent in the face of anything more ambitious. Russia could also resort to the use of tactical nuclear weapons to tip the balance in its favor. However, using such weapons would escalate the crisis, potentially trigger opposition from countries that have so far remained neutral, and have an environmental impact on Russia itself. Short of a massive Ukrainian breakthrough, the use of nuclear weapons thus seems unlikely. At the same time, there is little evidence that President Putin has any desire to end the conflict unilaterally, and several analysts believe he is keen to see what effect winter has on European's resolve to maintain sanctions and support Ukraine.

If Russia is unlikely to unambiguously 'win' or quit, therefore, the conflict will continue into 2023. It seems more probable that a 'steady state' will emerge, with Ukraine making incremental territorial gains, as happened in Kharkiv in September and Kherson in November. Russia will occasionally have its own small successes, but neither side will achieve decisive success. In place of major battlefield changes, Ukraine will continue to undertake spectacular 'behind the lines' attacks, such as the October 8 attack on the Crimean Bridge, and Russia will continue to launch missile and drone attacks on Ukrainian infrastructure and civilians. At some point, moreover, serious talks about ending the war will come, but again, it is unlikely that either side will be willing to make major concessions at this stage.

How will this affect western sanctions? It seems improbable that there will be any further EU move on natural gas supplies or an attempt to remove all Russian financial institutions from the international financial architecture unless prompted by a major escalation in Russian violence. New sectoral categories will probably be added in successive packages.

More generally, we are likely to see new sanctions focus on extending lists of designations for pre-existing types of targets, shortened timetables for the implementation of some existing bans, and a strong focus on tackling sanctions evasion efforts through new designations and law enforcement and judicial action, as well as the practical implementation of 'freeze to seize' measures. But 'freeze to seize' will take time to bear fruit, given that the legal basis for sustainable rather than ad hoc action does not yet exist in the US, Canada, the UK, or the EU, and the process of democratic legislation is typically slow.

It is likely that - paradoxically - we will also see some small and limited scaling back of western sanctions in some areas, even as the number of designations overall will continue to rise. Any successful legal action by an oligarch to have their name removed from sanction lists will set a precedent to cause major problems for the western approach.

Russia is also likely to seek concessions on sanctions as rewards for good behavior if talks develop. Indications of this are already evident from the reported request from November that Russia has made to western countries to remove the designation of the Russian state agriculture lender, Rosselkhozbank, to allow it to facilitate the export of Russian foodstuffs that could help ease global food supply chain problems. Such seemingly innocuous 'goodwill' quid pro quos are likely to grow, especially around energy supplies, and some will almost certainly be accepted. How many and how significant they will be at this stage, but the variables most likely to affect western governments' calculations will be how cold, and hungry their citizens feel by spring 2023.

What does this mean for your firm?

Our survey showed that 53 percent of firms have changed their business model in response to Russia's invasion. 50 percent have implemented asset freezes, and 44 percent introduced an onboarding shutdown. Just two percent of firms told us the invasion had no impact on their business.

It's clear, therefore, that compliance and sanctions teams have not underestimated how significantly the war in Ukraine can - and will - impact their businesses. But firms should always be prepared for further changes to the lists of Russian sanctions designations and should have appropriately comprehensive and agile screening tools in place. In our survey, 96 percent of firms told us real-time AML risk data would improve their response to sudden sanctions regime changes, like those seen in the case of Russia. Having identified the need, they should ensure they work with vendors that can deliver for them. Firms must ensure they do not take a minimalistic approach to detecting potential Russian sanctions exposure, especially since western government agencies will be increasingly focused on improving private sector implementation and reducing evasion.

Alia Mahmud
Regulatory Affairs Practice Lead, ComplyAdvantage

How has Russia's invasion of Ukraine impacted your organization's business?

Changed our business model

Implemented asset freezing

Onboarding shutdown in Russia

There has been no change

Source: ComplyAdvantage, State of Financial Crime 2023

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 Financial 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 (primary sanctions), the US also imposes sanctions on non-US citizens and entities engaging with designated targets (known as secondary sanctions). The US maintains the most extensive body of sanctions in the world, and has been an innovator in applying them to new challenges such as human rights abuses, for example, passing the Global Magnitsky Act in December 2016, named after accountant, Sergei Magnitsky, who died from mistreatment in a Russian prison in November 2009.

Iran

While Russia's invasion of Ukraine has been the primary focus for sanctions developments in 2022, other long-term targets of both UN and national sanctions have continued to generate concerns. Amongst the most prominent is the Islamic Republic of Iran, where the most enduring issue has been attempting to revive the partially moribund agreement on the limits to Iran's nuclear program, known as the Joint Comprehensive Plan of Action (JCPOA). However, progress has been soured by the re-emergence of old western concerns about Iran's human rights record, domestic repression, the funding of terrorism, as well as its links to the Russian war effort. Concern about Iran rose in this year's survey, with the country overtaking Afghanistan to become one of the top four geopolitical hotspots firms are concerned with.

Four Decades of Sanctions

Iran has been the target of a range of US sanctions since 1979, when its then ruler and US ally, the Shah, was overthrown by an Islamist extremist revolution led by Ayatollah Khomeini. Although the US was at the outset most concerned about the treatment of US hostages taken by the new regime (all were subsequently released by January 1981), it has since focused on a wide range of other alleged Iranian misdemeanors, including state terrorism and overseas interference by the Iranian intelligence services and the Iranian Revolutionary Guard Corps (IRGC), support for Islamist groups such as Hezbollah and Hamas, human rights abuses at home, cyber criminality, and most controversially, Iran's attempts to develop military nuclear technology and ballistic missiles. US sanctions in response have been wide-ranging, seeking to freeze Iranian assets, ban Iranian involvement in the US-dollar-denominated financial system, and eliminate Iran's capacity to sell its primary national commodities, oil, and gas, and other petrochemicals, as well as targeting key regime figures with asset freezes and transactional and travel bans.

Although much has been distinctive to the US approach, the wider international community has shared the US's concern over Iran's Weapons of Mass Destruction (WMD) program. From July 2006, the UNSC adopted a range of measures to encourage the Iranians to stop their programs, such as a blanket asset freeze and logistical designations to prevent procurement and proliferation. The EU, Canada, the UK, and others also joined the US in condemnation of Iranian nuclear ambitions and human rights abuses, with the EU imposing its own measures on Iran's financial, energy and transport sectors, including a ban on the import of Iranian oil and gas. In March 2012, the EU - with US encouragement - also required SWIFT to remove sanctioned Iranian financial institutions from the service, effectively freezing Iran out of the global financial system.

Elements of the US, EU, and UN regimes linked to Iran's nuclear program were partially lifted in July 2015 as a result of the conclusion of the JCPOA, signed by Iran and the five permanent UNSC nations plus Germany and the EU. Under the JCPOA, Iran was allowed access to the international financial system and to re-engage in global markets for key commodities such as oil and gas in return for limits on uranium enrichment. However, the Trump administration withdrew from the agreement in May 2018, citing Iranian breaches to the agreement and malign interference in neighboring countries such as Iraq, and reimposed US sanctions later that year. Although the other parties remained, and Trump's successor Joe Biden supported talks to revive the deal under the auspices of the International Atomic Energy Authority (IAEA) in Vienna, as of the start of 2022, the fate of the JCPOA remained uncertain.

2022 Developments

Ironically, for a year that began with hopes of improving US-Iranian relations and alleviating sanctions, events have taken a different direction. Throughout the year, talks in Vienna made progress, and by early August 2022, Josep Borrell, the EU High Representative for Foreign Affairs and Security Policy, tweeted that a draft agreement was on the table. But both the US and Iran were more circumspect, with Iran insisting that there be stronger guarantees that the country would retain economic sanctions relief if a future US president withdrew from the agreement again and calling for the end to an ongoing IAEA investigation into alleged Iranian breaches. By mid-September, moreover, Borrell was also less positive, saying that the talks were at a point of "stalemate."

The block on progress came from the inherent challenge that the talks were certainly affected by the long-term antagonism between the US and Iran, but contextual issues also played a role. Some were short-term; in the US, mid-term congressional and gubernatorial elections on November 8 made it difficult for the Biden administration to make compromises with Tehran that might lead to Republican criticism. Others were more concrete and long-term. Iranian military interference across the Middle Eastern region continued, including IRGC missile strikes against claimed Israeli targets in northern Iraq and against a Saudi Aramco facility in Yemen by Iranian-backed Houthi rebels, both in March 2022. Further points of contention between Iran, the US, and its allies emerged in the second half of 2022.

One was the death in custody on September 16 of the 22-year-old Kurdish Iranian, Mahsa Amini, who had been arrested by the Gasht-e Ershad, the Iranian Morality Police, for allegedly violating dress rules. Her death - which the police claimed was due to an underlying health condition, but others suggest resulted from brutal treatment - led to widespread outrage in Iran and successive mass protests across the country. The Iranian regime reacted with force to these protests, deploying riot police, arresting protest leaders, and placing restrictions on social media usage.

The other was Iranian support for Russia's invasion of Ukraine, which at the outset was largely rhetorical. Iranian President Ebrahim Raisi quickly informed President Putin that he understood and shared Russia's security concerns despite widespread international condemnation. However, over the year, evidence mounted that Iran was providing more practical military support to Russia in the form of Shahed-136 military drones, which Russia used in attacks on the Ukrainian military and infrastructure, as well as military advisers to enable the weapons' deployment.

Sanctions Response

In light of the overall lack of progress in the nuclear talks and the general worsening of Iranian-western relations, 2022 thus resulted in the continuation and extension of a range of existing sanctions on Iran, especially those imposed by the US:

- **Weapons Proliferation**: Following missile strikes in March, the US designated Iranian national Mohammad Ali Hosseini and a network of linked companies for procuring ballistic missile propellant on behalf of the IRGC. The OFAC designation stated that the propellants had been sourced from China using false shipping documentation.
- **Oil Sales**: In June, July, August, September, and November 2022, OFAC sanctioned individuals and front companies operating as networks for the sale of Iranian oil and other petrochemicals in East and Southeast Asia. The designations suggested a wide geographic scope for these networks, with nodes in China, Hong Kong, Malaysia, and UAE. In the November designations, OFAC stated that the oil trading was specifically intended to support the IRGC's elite 'Quds Force' and Hezbollah.
- **Cybercrime**: In September 2022, the US sanctioned the Iranian Ministry of Intelligence and Security (MOIS) and the Minister of Intelligence, Esmail Khatib, for mounting Iran's campaign of cyber and ransomware attacks, including a 2022 identified attack against the Albanian government. A further OFAC designation in September targeted several Iranian nationals and Iran-based companies linked to IRGC ransomware attacks. Separately, a blog post by blockchain analytics firm Chainalysis in September identified several sanctioned users of Iran's largest cryptocurrency exchange, Nobitex. According to the report, over $230,000 in Bitcoin generated from ransomware attacks was sent to digital wallets held by the sanctioned Iranians at Nobitex between 2015 and 2022.

From September onwards, the US, EU, Canada, and the UK announced a range of sanctions targeting the Iranian Morality Police, its leadership, and other Iranian agencies such as the Law Enforcement Forces (LEFs) involved in domestic repression. In parallel, the US, EU, Canada, and the UK took further coordinated action against Iranian support for Russia, designating Iranian companies and individuals involved in the development, manufacture, and supply of the Shahed drone series being deployed by Russia in Ukraine.

Of these two areas of western action, the one which appears to have had the most apparent impact on Iran has been the measures announced against domestic repression. The Iranian Ministry of Foreign Affairs condemned the designations in October and took the unusual step of issuing its own counter-sanctions against entities and individuals in the EU and UK. Those targeted included civil society groups, media groups, politicians, and journalists, which the Iranian government argued were "provoking riots, violence, and terrorist acts" in Iran.

Prospects for 2023

Overall, the prospects for Iranian relations with the US and other western countries in 2023 look poor. Positive developments in the Vienna talks remain possible, but the relative gloom of optimists such as EU foreign affairs lead Josep Borrell suggests that they are unlikely. There is considerable distance still between the US and Iran, and in light of the wider political context, the EU and UK seem unlikely to encourage the US to take a risk. The Biden administration will also be increasingly cautious about doing so as of 2023, with Congress finely balanced between the parties and a presidential election coming in November 2024. President Biden will not wish to give his potential opponents a stick with which to beat him or encourage a newly installed hawkish Israeli government under Binyamin Netanyahu to consider using military force against Iranian reactors. It is unlikely that the JCPOA will be revived in 2023.

On the contrary, 2023 looks more likely to lead to a hardening of the western position against Iran, with the EU, Canada, and the UK moving progressively towards a more hard-line position. The Iranian government's crackdown on its people and its support for Russia are two areas of significant concern that are likely to lead them to continue coordinating further new designations in these areas with the US. There is also the possibility that some western countries will take more action in areas where the US has previously acted alone, such as Iranian support for terrorism. The UK is the likeliest case for future action in 2023, given comments in November 2022 by Ken McCallum, Director General of the UK's domestic intelligence agency MI5, that Iran had been behind ten plots to kill or kidnap individuals in the UK.

What does this mean for your firm?

"Those firms with potential Iranian sanctions exposure risk should expect no change. Businesses will need to maintain effective due diligence and screening measures, and those based in areas used as locations for Iranian clandestine procurement and commodity trading - in particular the Middle East, East and Southeast Asia - will need to take care to mitigate risks from Iranian evasion activities using proxy front companies."

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

North Korea

Alongside Iran, North Korea (officially the Democratic People's Republic of Korea, or DPRK) is the most intractable problem in international affairs and one where sanctions have been applied even more intensively. Like Iran, it is a problem that has continued to bring challenges in 2022. The regime of Kim Jong-un continues to flaunt its UN-designated WMD program, evade sanctions, and generate money via cybercrime. Like Iran, it, too, has provoked western anger by providing material support to Russia's invasion of Ukraine.

Sanctioning the Hermit Kingdom

North Korea has primarily been subject to US sanctions, which were first initiated with the outbreak of the Korean War in 1950, and have continued in various forms since, targeting conventional weapons proliferation, terrorism, overseas political interference, illegal activities such as drugs trafficking, counterfeiting, smuggling, cybercrime and money laundering, human rights abuses, and WMD development. As a result, 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.

Although the US has been the primary designator of North Korea, the wider international community has shared US concerns with regard to North Korean WMD efforts. Following North Korea's first successful nuclear test in October 2006, the UNSC imposed initial sanctions under Resolution 1718 and a succession of further resolutions seeking to limit North Korea's ability both to procure items to support the building of nuclear weapons and ballistic missiles, but also to finance those activities through legitimate trade and overseas money-making schemes, both licit and illegal. Over the last decade or so, Japan, South Korea, Australia, the EU, the UK, and Canada have also followed the US in introducing additional autonomous sanctions against North Korea chiefly related to nuclear weapons proliferation, but also some individual issues such as historic abductions of Japanese citizens.

2022 Developments

The two 2022 reports of the UN Panel of Experts (PoE) on North Korean sanctions, published in March and September, indicated that the North Korean regime had continued its clandestine proliferation activities, both in the face of sanctions and the country's own border closure, which began in January 2020 in response to Covid-19. Following the pattern of findings in previous reports, the PoE found that North Korea had sourced sanctioned items necessary for its WMD programs, bought and sold goods such as oil and coal beyond UN limits, and generated hard currency through money-making schemes, including the provision of illegal labor. These activities are managed by North Korea's diplomatic and official presences, as well as complex webs of front companies and logistics firms and vessels based across numerous jurisdictions, which were used to obfuscate links back to the North Korean state and the secretive Offices 38 and 39, alleged coordinators of overseas activities.

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.

The reports also noted the increasing reliance of North Korea on state-sponsored cybercrime. According to the reports, North Korea uses around 6,000 hackers in different operational units, such as the so-called 'Lazarus Group,' operating both from Pyongyang and parts of Southeast Asia, under the general guidance of the state Reconnaissance General Bureau (RGB). Their activities seemed to be heavily targeted at stealing cryptocurrencies, using a range of phishing, malware, and social engineering techniques. Using figures produced by Chainalysis, the PoE estimated that North Korea had stolen the equivalent of $400 million in cryptocurrency in 2021, a significant rise on 2020. The PoE (following the US's lead) also identified North Korea as the likely culprit behind two major hacks in 2022; in March, North Korea's hackers stole the equivalent of around $650 million in Ethereum and USD Coin from Ronin Network, a platform supporting the mobile game Axie Infinity, and in June, the equivalent of around $100 million was taken from Harmony Horizon, a cross-chain bridge which allows migrating assets between several major blockchains, using similar methods to the Ronin attack.

More publicly, North Korea has also continued to attempt to demonstrate the fruits of its proliferation efforts throughout the year, with numerous tests of ballistic weaponry. In March, the regime announced it had successfully launched its largest Intercontinental Ballistic Missile (ICBM), the Hwasong-17, allegedly capable of hitting anywhere in the continental US. This was the first test of an ICBM since 2017, although subsequent analysis suggested it might have been a smaller missile, the Hwasong-15. Several other ICBM tests were claimed across the year, including one in November, which fell in the Sea of Japan, close to the Japanese island of Hokkaido. North Korea also tested a range of other missiles, from short, medium, to intermediate, which could be used in battlefield situations and to attack its neighbors, Japan and South Korea. According to an analysis by Al Jazeera in November, North Korea tested over 60 missiles in 2022, the largest number of missile tests it had ever conducted in one year. The increased volume of tests led some, including the South Korean government, to suspect that North Korea was preparing to conduct its seventh nuclear test, the first since 2017.

In addition to these provocative actions, North Korea has also allegedly joined Iran in providing material support for the Russian invasion of Ukraine. In July, there were discussions of theoretical collaboration when the Russian Ambassador to Pyongyang suggested that North Korean labor could be used to rebuild Donbas and Luhansk. By the autumn, however, it was clear that North Korean support was probably more immediate, with reports emerging that North Korean factories were producing military uniforms for Russia and that the country was supplying the Russian army with Soviet-era munitions.

Sanctions Response

The UNSC response to North Korea's recalcitrance in 2022 has been non-existent, with numerous recommendations of further actions from the PoE unmet. In May 2022, the US put forward a new UNSC resolution on North Korea, intended to tighten sanctions further in specific response to North Korea's ballistic missile tests. However, despite support from European countries, the resolution was not passed in the face of vetoes from China and Russia. According to the Chinese ambassador to the UN, further sanctions would "lead to greater tensions," while the Russian deputy ambassador explained he feared "humanitarian turbulence" as a result of new measures. Although this was the first overt split of the UNSC on North Korea since the introduction of UN sanctions in 2006, it reflected the growing differences in approach between the western permanent members versus Russia and China, who had already failed to agree on any new UN North Korea resolutions since 2017.
As a consequence, new sanctions in response to North Korean activities came at a national level, primarily from the US, around a number of key themes:

- **Missile Procurement:** In January, April, and May, OFAC designated a number of entities and individuals for involvement in procuring items for WMD and ballistic missile production. These included the North Korean Ministry of Rocket Industry (MoRI) and several supporting trading companies, and North Korean nationals based in Russia and China. In addition, OFAC sanctioned two Russian financial institutions, Bank Sputnik and Far Eastern Bank, and a Russian national for supporting North Korean procurement and proliferation financing. In February, the BIS also placed export controls on a Chinese firm for supplying North Korea with aluminum powders that could be used in ballistic missile propellants.

- **Fuel Procurement:** In October, OFAC designated a group of three individuals - Singaporean, Malaysian, and Taiwanese - along with four companies based in Singapore, Malaysia, and the Marshall Islands for supporting petroleum exports to North Korea using ship-to-ship transfers. One of the individuals, Singaporean Kwek Kee-Seng, was also wanted in an FBI-led investigation of economic sanctions evasion and money laundering.

- **Cybercrime and cryptocurrency theft:** In May, OFAC designated Blender, a cryptocurrency mixing service, after the Lazarus Group used its services to launder $20.5 million of the funds stolen in the Ronin Network hack. It was the first designation of its type. In August, a further mixing service, Tornado Cash, was also designated after OFAC identified it as a platform used by criminals to launder funds, including $455 million taken by the Lazarus Group. Further North Korean-related cyber designations were made throughout the year, including two Chinese nationals linked to the Lazarus Group in March and several Ethereum addresses linked to laundering funds from the Ronin Network hack in April.

But the US has not been alone in taking action, and several of its allies also added additional measures in the face of ongoing North Korean activities and the stalemate in the UNSC. In April, the EU imposed sanctions on eight North Korean nationals, including senior officials and individuals involved in proliferation activities in sub-Saharan Africa. Several entities were also listed, including three North Korean state trading corporations, as well as an Eritrean technology firm. The UK made several additions to its own North Korean list across the year, including North Korean nationals, a North Korean trading corporation, and a Chinese logistics firm. Australia added three entities to its autonomous regime - one North Korean and two Russian - following the missile test of March, and Japan also added five North Korean state entities linked to weapons development to its own North Korean sanctions following the ICBM test in October.

Prospects for 2023

North Korea is highly likely to carry on its current path in 2023, with further missile tests and proliferation activities. Having built up a significant cyber-crime capability in recent years, it will also continue to launch cryptocurrency heists. However, a prolonged fall in the value of cryptocurrencies might lead to a switch in tactics and a return to focus on stealing fiat currencies, along similar lines to the North Korean attempt to steal $1 billion of the Federal Reserve Bank of New York's accounts with Bangladesh Bank in February 2016.

There is little prospect for any improvement in the standoff between western countries and North Korea. The likeliest development will be a further worsening of the situation, triggered by any one of a number of North Korean acts, from the testing of a nuclear device, further missile launches close to South Korea and Japan, or more open and extensive support for Russia in Ukraine. With the possible exception of a new nuclear test, none of these events will lead to a new resolution at the UNSC because of the block now placed by China and Russia. This indicates that further measures will probably come from western national regimes alone. For the US, with its pre-existing package of comprehensive North Korea sanctions, new additions are likely to be focused on the expanding area of North Korean cybercrime and cryptocurrency theft. The US is also likely to look ever more closely at third-country support for North Korean evasion efforts, especially in China and Russia. The EU, UK, Australia, and Japan will also augment their own lists in 2023, with a North Korean nuclear test likely to stimulate the widest range of action.

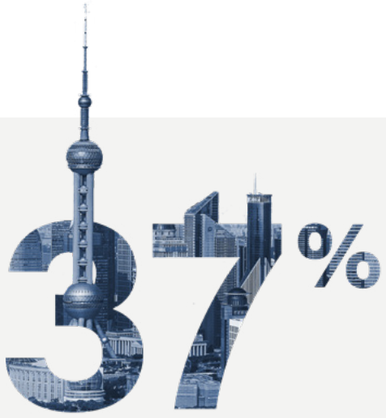
What does this mean for your firm?

"US and US-exposed firms will already be aware of the extensive nature of US-North Korean sanctions coverage, but they should continue to watch for list updates in 2023, especially concerning cryptocurrency designations. The US's decision to target two mixers alleged to have facilitated North Korean cryptocurrency money laundering suggests that all CASPs will need to look carefully at their own due diligence, scanning, and monitoring procedures to ensure that they, too, do not fall foul of OFAC. Ignorance will not be a valid defense."

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

China

In our State of Financial Crime 2022 report, we identified China as the greatest area of concern for new sanctions risk. However, the crisis in Ukraine partially eclipsed these concerns in 2022, and China has maintained a careful position on the invasion, balancing a broadly pro-Russian stance with expressions of support for peace. Chinese domestic preoccupations have had an effect, too, with Beijing focused on managing Covid, and consolidating President Xi's power with his appointment to a third term, agreed at the Chinese Communist Party's 20th Congress in October. Nonetheless, underlying frictions with western countries remain, especially over the status of Taiwan, which China sees as an integral part of the country despite the island's long-running de facto independence. That's why, despite a five percentage point drop, China remained a concern for 37 percent of organizations.



of organizations say China is the hotspot they're most concerned about

Source: ComplyAdvantage, State of Financial Crime 2023

The Struggle for Global Leadership

The geopolitical context of western sanctions against China is the country's rise to global political and economic pre-eminence over the last forty years. Since 2000, Chinese GDP has grown from $1.2 trillion to $17.7 trillion, making it the second largest economy in the world after the US and likely to become the largest within a decade. This growth is not a problem in itself, and China, heavily integrated into the global economy, has been a proactive partner in trade with western countries. However, the US and its allies have become more concerned in the last decade with how this economic strength has enabled the projection of Chinese influence across Asia, Africa, and Europe via the Belt and Road trade initiative, the growth of a technologically sophisticated Chinese military, and Chinese attempts to expand its zones of control around the small island chains of the South and East China Seas.

In addition, western governments have expressed disquiet at the Chinese government's increasingly draconian domestic surveillance measures, the persecution of minorities such as the Muslim Uyghurs of Xinjiang, and the undermining of civil liberties in Hong Kong, a Special Administrative Region of China with control over its own internal governance.

The US and its allies have come together over the last decade to find ways to counterbalance China, using mechanisms such as the 'Five Eyes' group, the Quadrilateral Security Dialogue, known as the 'Quad' formed in 2004 by the US, Japan, Australia and India, and the AUKUS partnership of Australia, UK, and the US, formed in 2021. A large part of this activity has focused on the coordination of military and intelligence activities to meet the Chinese challenge, however, leaving tools of economic statecraft to one side.

This has left the US to take the lead - once again - on the use of sanctions as a means of international influence against the Chinese. The US application of sanctions has a long history, with the country applying a trade embargo for over twenty years following the Communist victory in the Chinese Civil War in 1949 and an ongoing arms embargo after the crackdown on protests at Tiananmen Square in 1989. However, the greater part of the contemporary US framework of China sanctions has taken shape through the Trump and Biden presidencies.

Its key pillars included measures on:

- **The Chinese Military-Industrial Complex:** In November 2020, President Trump signed an Executive Order which prevented US citizens and entities from investing in companies designated by the US Department of Defense (DoD) as Communist Chinese Military Companies (CCMCs). In June 2021, President Biden signed an updated Executive Order which expanded the range of companies that could be deemed to be supporting the Chinese military-industrial complex, Chinese overseas activities, and domestic repression.

- **The Chinese Telecommunications Sector:** In May 2019, President Trump signed an Executive Order banning the use of equipment from Chinese technology firms deemed a national security risk. Subsequently, a number of Chinese technology firms, such as Huawei, were placed on the BIS Entity List. The exclusion of Chinese telecommunications firms from the US was further entrenched by the Secure and Trusted Communications Act of 2019 and the Secure Equipment Act of 2021.

- **Human Rights Abuse of the Uyghurs:** In June 2020, President Trump signed the Uyghur Human Rights Policy Act, which authorized the president to designate Chinese individuals responsible for the persecution of the Uyghurs using the US's Global Magnitsky legislation. The Trump administration subsequently sanctioned numerous senior Chinese officials, including Politburo member Chen Quanguo. In December 2021, President Biden signed the Uyghur Forced Labour Prevention Act, which prevented the US import of goods made with forced labor in Xinjiang.

- **Human Rights Abuses in Hong Kong:** In 2019, President Trump signed the Hong Kong Human Rights and Democracy Act, and in 2020, the Hong Kong Autonomy Act, which provided the legal basis for the designation of Chinese and Hong Kong individuals responsible for human rights abuses, and those deemed to have undermined Hong Kong's autonomy. The latter act led to the designation of a number of senior Hong Kong officials, including its then Chief Executive, Carrie Lam. The act also included provisions for the designation of Foreign Financial Institutions (FFIs) providing material support to targeted individuals.

Although the US was the prime mover in developing a wide-ranging sanctions response to Chinese activities before 2022, there were indications that several of its allies were starting to follow its lead, especially with regard to confronting Chinese human rights abuses in Xinjiang. The EU, the UK, and Canada imposed similar, coordinated measures in the spring of 2021 against Chinese officials complicit in the persecution of the Uyghurs.

At the same time, China responded to these measures with a succession of targeted designations against US, EU, UK, Canadian and Taiwanese officials and politicians in 2020 and 2021. It also took aim at Australian criticisms of its human rights record in 2020 with the imposition of huge tariffs on a range of Australian imports and withdrew its ambassador from Lithuania when the country announced in November 2021 that Taiwan would open a trade office in the Lithuanian capital, Vilnius.

In addition, China continued to lay the groundwork for a comprehensive sanctions regime targeted at foreign businesses, beginning with the creation of an 'Unreliable Entities List' (UEL) in 2020 and followed in 2021 by the creation of a Blocking Statute and an Anti-Foreign Sanctions Law (AFSL). Taken together, this package of measures allowed the Chinese Ministry of Commerce (MOFCOM) to designate foreign firms deemed a risk to Chinese national security and to block firms operating in China from complying with foreign (i.e., US) sanctions targeted on Chinese businesses. Until the end of 2021, the measures had only limited usage, apart from a threat in October 2020 to add western defense firms such as Lockheed Martin and Raytheon Technologies to the UEL for supplying defense equipment to Taiwan.

Although the US was the prime mover in developing a wide-ranging sanctions response to Chinese activities before 2022, there were indications that several of its allies were starting to follow its lead

2022 Developments

Despite the darkening background of relations between western countries and China, tensions - while present - have been largely contained in 2022. Allegations of mistreatment of Uyghurs in Xinjiang have continued to generate angry diplomatic exchanges between both sides, occasioned this year by an official boycott of the Winter Olympics by the US and others in February and a report by the then UN Human Rights High Commissioner issued in August, which assessed that the treatment of the Uyghurs potentially amounted to "crimes against humanity." However, the level of argument between China and the democratic coalition over human rights issues has 'simmered' rather than boiled in 2022.

A similar assessment can also be made of the democratic community's reaction to China's ongoing warm relationship with Russia. Speaking in March, President Biden told President Xi that there would be "consequences" for Chinese "material support" of the invasion, a threat to which Xi has apparently paid heed. China has thus been extremely careful not to condemn Russia, stressing the importance of state sovereignty - both Russia and Ukraine's - and the need to find peace. Where blame has been laid, China has primarily looked at the West, particularly the role of NATO expansion, in causing legitimate security fears in Russia. At the same time, US intelligence reports indicated in July that the Chinese government had shown no signs of providing economic, financial, or military support for Russia or seeking to help evade western sanctions against Russia.

The one area where tensions have been most obvious has been Taiwan, the island to which the Chinese Communists' civil war opponents, the Kuomintang, retreated in 1949. Although not recognized as an independent state by the US or other western states since 1979, it does receive western support in the face of Chinese demands that it re-integrate with the mainland as part of Beijing's 'One China' policy. 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.

The issue came forward once again in May when President Biden said in Tokyo that while respecting China's views, he would use military force to defend Taiwan. In response, the Chinese Foreign Ministry expressed "strong dissatisfaction." Matters escalated significantly several months later when the then Speaker of the US House of Representatives, Nancy Pelosi, visited Taiwan on August 5 to show her support for the island. In response, China canceled ongoing security dialogues with the US and mounted large-scale military exercises around Taiwan. Chinese anger remained high into the autumn, with Xi telling the Party Congress in October that China reserved the right to use "all necessary measures" in dealing with Taiwan. Nonetheless, by year-end, matters had calmed enough for Presidents Biden and Xi to meet at the G20 Summit in Bali in November, where - despite frank discussions - readouts appeared to indicate a cooling of tempers.

Sanctions Response

In light of the broader geopolitical environment, western sanctions activity against China has been relatively muted in 2022. In March, the US Department of State placed visa restrictions (but not financial sanctions) on several Chinese officials alleged to have been involved in domestic repression, and in June, the Uyghur Forced Labor Prevention Act, passed in December 2021, came into effect. The EU, UK, Canada, and others also took few additional measures on human rights issues in China in 2022, despite pressure from civil society groups following the publication of the UN report in August.

As noted above, the US took further action against several Chinese firms in the context of sanctions evasion activity linked to Iran and North Korea, and in June, the BIS added 36 firms to its Entity List for aiding Russian sanctions evasion, 25 of which had China-based operations, and five of which were Chinese incorporated businesses. However, the US also indicated that it did not believe that these companies were acting for the Chinese government.

The area of most significant US sanctions activity against China in 2022 was technology. In February, the BIS added 33 China-based companies, mostly in areas such as semiconductors, laser technology, pharmaceuticals, and advanced research, to the BIS Unverified List (UVL), which indicates uncertainty about the end-use of exported goods, requiring further due diligence from US exporters. In August, BIS added a further seven Chinese firms in space and aerospace technology to its main Entity List, and in October, issued new regulations prohibiting the US and US-based companies from exporting to China advanced chips and software related to machine learning. The regulations also banned covered businesses from manufacturing advanced chips for Chinese firms, affecting the operations of some of the world's largest technology companies, such as the South Korean Samsung.

China's deployment of its own sanction regime in response was also circumspect in 2022 and focused primarily on Taiwan. Following her trip to Taiwan, the Chinese Ministry of Foreign Affairs announced personal sanctions on Nancy Pelosi and her immediate family members, and also a mid-ranking Lithuanian minister who visited Taiwan in the same month. China also continued to target US defense firms that had provided equipment for the government of Taiwan. In February, China made new threats to sanction Raytheon and Lockheed Martin, following the announcement of a $100m deal to upgrade Taiwan's missile defense systems, and in October, said that personal sanctions would be applied to the CEOs of Raytheon and Boeing Defense following a new arms deal with Taiwan. However, the Chinese government made no sweeping designations of the US or other firms in response to technology controls or other previous measures in regard to Xinjiang or China.

Prospects for 2023

After a tumultuous 2021, 2022 was a difficult but more tempered year in Chinese-western relations. Neither side seems to wish to add additional disruptions to the current crisis in Ukraine. Both sides also appear aware of the complexity of their economic interrelationship. Unlike Russia, China is central to the global economy's health for all parties. Going beyond certain carefully calibrated limits in imposing sanctions - in either direction - is likely to generate a mutually detrimental downward spiral.

This perhaps helps explain, amongst other factors, why, after the volley of western action with regard to Chinese human rights abuses in 2020 and 2021, few new human rights-related sanctions were imposed in 2022, even in the face of a damning UN report. It is probable that while there will be further western sanctions on Xinjiang and Hong Kong in the future, these are likely to be incremental additions. Chinese counter-designations are likely to be limited 'tit-for-tat' individual designations of politicians, officials, and civil society groups that criticize its behavior.

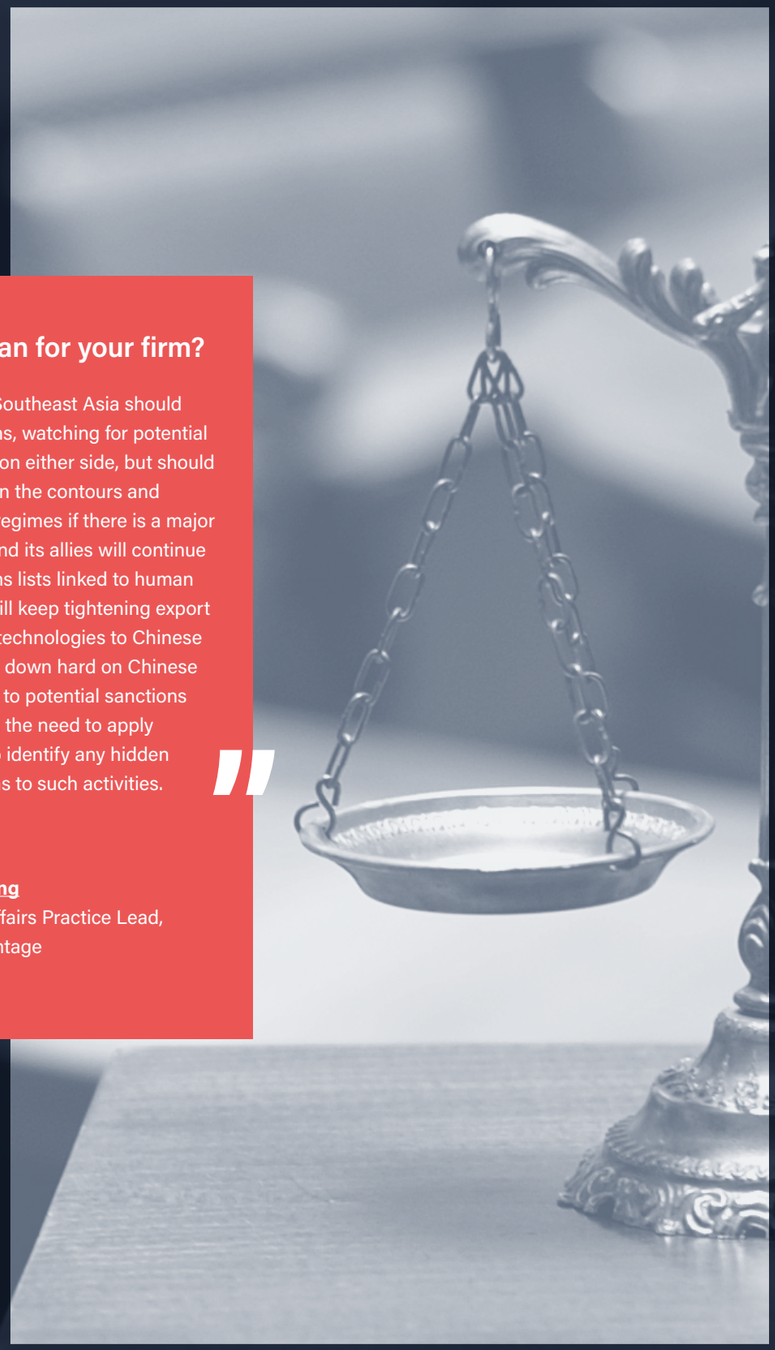
However, perceived national security concerns still matter, and 2023 will likely see an expanding range of technology and related sanctions against China by the US. Other western countries joining the US in imposing blanket measures seems unlikely, although the UK and other 'Five Eyes' countries which have expressed concerns about Chinese industrial espionage may do so in the future. In parallel, Chinese sanctions against the democratic coalition are likely to be focused on explicit political and material support for Taiwan. More wide-ranging counter-sanctions using the Chinese sanctions laws against US technology businesses seem unlikely in the current environment.

The key factors which could cause a change in this situation in 2023 are China's position on Ukraine and Taiwan. If China were to begin providing significant material support to Russia, then the US, EU, UK, Canada, and others would begin targeting Chinese firms, government bodies, and officials suspected of being directly involved in providing support, although targeted sanctions of senior Chinese figures or major government departments seems highly unlikely. Such western sanctions would be highly calibrated and carefully chosen and intended to be consequential but not provocative.

Taiwan would present a different challenge, however, with the democratic coalition's response varying with the nature of Chinese action. Rhetorical threats to re-integrate Taiwan into China would be largely ignored, but military preparations or a blockade of the island would probably lead to coordinated western sanctions on sectors linked to defense, technology, but also transport, and logistics, as well as targeted sanctions against more senior figures in the Chinese government. In the event of an invasion, additional measures would mirror sanctions against Russia, such as excluding some Chinese financial institutions from the international financial system and caps on oil and gas sales and other energy commerce. The US would also impose secondary sanctions on FFIs that were deemed to be providing services to the Chinese state. However, if China does invade and makes relatively swift progress then the most pressing question will not be about sanctions but whether the US, Japan, and others will come to Taiwan's aid with military intervention.

Fortunately, these extreme scenarios seem unlikely. Given the stalemate on the ground in Ukraine, China has no obvious interest in changing its stance on providing material support to Russia. The only probable prompt for that is if China itself were subject to a major sanctioning effort similar to that against Russia, which would only arise in the face of a Chinese invasion of Taiwan. This prospect cannot be ruled out. Facing a West distracted with Ukraine and struggling economically, and with difficult domestic problems for which a successful war might bring distraction, President Xi might decide that the moment has come to 'reunite' China in 2023. However, this seems improbable, despite some of President Xi's bellicose remarks. Faced with a challenging situation at home, a decision to go to war with no immediate provocation would be a huge gamble.

As has long been the case, the likeliest trigger of Chinese military action would be a perceived provocation - specifically, a Taiwanese declaration of independence. This, too, seems unlikely under the current Taiwanese presidency of Tsai Ing-wen, who, despite taking a tough line on China, has yet to push hard on the issue of independence. Nor does she have a tide of domestic opinion currently encouraging her to do so. Although in office until 2024, Tsai resigned her position as leader of the Democratic Progressive Party (DPP) in November 2022, following local election losses to the more pro-Chinese opposition (the Kuomintang or KMT). 2023 will thus be a year of ongoing challenges between China and the West, but not one likely to lead to a change in the economic statecraft of either side.



What does this mean for your firm?

Firms exposed to East and Southeast Asia should monitor US-Chinese relations, watching for potential shifts in the tone of rhetoric on either side, but should only expect major changes in the contours and trends of current sanctions regimes if there is a major crisis over Taiwan. The US and its allies will continue adding incremental sanctions lists linked to human rights abuses, and the US will keep tightening export controls on firms supplying technologies to Chinese firms. The US will also come down hard on Chinese and Hong Kong firms linked to potential sanctions evasion in Russia, indicating the need to apply screening and monitoring to identify any hidden links to potential connections to such activities.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

Regional Review

Outside of the 'big four' targets of international and western sanctions, 2022 also saw developments in sanctions regimes against other countries and in the face of key thematic risks, which are reviewed below in digest form.

Europe

Relations between western countries and President Alexander Lukashenko of **Belarus** have been strained since he came to power in 1994 due to his repressive domestic measures and close relationship with Russia. Lukashenko, members of his regime and state institutions, and state-owned businesses have been subject to various measures by the US, EU, Canada, and the UK in the face of rigged presidential elections in 2006 and 2020, the violent suppression of public protests and the kidnapping of domestic dissident Raman Pratasevich and his girlfriend from an airplane in May 2021.

In February 2022, Lukashenko provided Russia with material support for its invasion of Ukraine, allowing Russian troops to be used as a base for operations. In response, successive western sanctions against Russia have featured restrictive measures against Belarus, including personal sanctions on members of the regime (the US redesignating Lukashenko in March, for example), transaction prohibitions with the Central Bank of Belarus, the removal of several major Belarusian banks from SWIFT, limitations on financial transactions, and restrictions on trade in key sectors such as defense and technology. In 2023, the imposition of new measures against Belarus will likely follow the same pattern as Russia, although they could widen and grow deeper if Belarus were to commit its own troops to Ukraine.

Although not directly linked to the Ukrainian situation, the US also looked to target Russia's European allies more widely in 2022. In October, OFAC designated nine corrupt politicians, officials and oligarchs, and a number of linked businesses in **Moldova**. These included several individuals with strong ties to the Putin regime, which, the US alleged, had worked to undermine Moldovan elections in 2021 on behalf of Russia.

In October, OFAC designated nine corrupt politicians, officials and oligarchs, and a number of linked businesses in Moldova. These included several individuals with strong ties to the Putin regime, which, the US alleged, had worked to undermine Moldovan elections in 2021 on behalf of Russia.

Beyond challenging Russian influence - although not totally unrelated, given Russian ties to local politicians - western countries also took action in support of the stability of **Bosnia and Herzegovina**. Existing US, EU, and UK sanctions have targeted corruption and individuals who have sought to undermine the Dayton Peace Accord of 1995, which ended the country's civil war. With Bosnia threatening to collapse into disorder once more in 2022, the US has taken action throughout the year, imposing measures on politicians, including the Bosnian Serb leader Milorad Dodik and the President of the Bosniak-Croat federation Marinko Cavara, alongside corrupt state officials and business people. In March, the EU decided to continue its current sanctions regime until March 2024, and in April, the UK imposed sanctions on Dodik and Zeljka Cvijanovic, currently the Serbian representative in Bosnia's federal presidency. Following a general election in October, extreme nationalist politicians have retained their primary positions, leaving the situation precarious and making further designations in 2023 likely.

Asia

Myanmar has remained a jurisdiction of significant concern in 2022. Following a military coup in February 2021, western governments called for the release of the overthrown leader, Aung San Suu Kyi, and the end of repressive measures against protestors. Sanctions action was blocked at the UNSC, primarily by China, but through the following weeks and months, the US, EU, Canada, and the UK imposed targeted designations on senior military leaders, state-owned enterprises, and companies in key sectors for Myanmar's economy, including the timber trade and mining.

The Financial Action Task Force (FATF), the international standard setter on financial crime, added Myanmar to its list of 'High-Risk Jurisdictions,' putting it in the same category as international pariah states like North Korea and Iran.

In 2022, the US and others continued to impose new sanctions on the military regime and its private sector supporters, with the EU marking the anniversary of the coup in February with a range of measures, including the designation of the state-owned energy firm, Myanma Oil and Gas Enterprise (MOGE). The Myanmar military regime has also faced widespread international criticism for the ongoing persecution of Aung San Suu Kyi, who was placed on trial in 11 separate corruption cases. In the first trial, she was found guilty in April 2022 and imprisoned for five years. In response to what it sees as "politically motivated" prosecutions, the US took specific action against figures in law enforcement and the judiciary in January. The US also took note of Myanmar's drawing closer to Russia over the year and, in October, designated three Myanmar businessmen as well as their business for buying Russian-produced arms for the regime.

By the close of 2022, Myanmar's isolation from the international community, save from Russia and China, had clearly increased significantly. In October, the Financial Action Task Force (FATF), the international standard setter on financial crime, added Myanmar to its list of 'High-Risk Jurisdictions,' putting it in the same category as international pariah states like North Korea and Iran. With no obvious prospect of the Myanmar regime changing course in the near future, it seems likely that the US and others will continue to tighten sanctions in 2023, especially following further guilty verdicts in the forthcoming trials of Aung San Suu Kyi and any indications of material support for the Russian invasion of Ukraine.

In light of Ortega's apparent unwillingness to reform - reflected in further rigged municipal elections in November 2022, as well as Ortega's public support for the Russian invasion of Ukraine - 2023 looks likely to be a year in which sanctions are tightened further.

Americas

Since 1979, President Daniel Ortega has been a dominating political figure in **Nicaragua**. The national leader between 1979 and 1990 and again from 2007 onwards, Ortega and his associates in the leftist Sandinista movement established tight control over the levers of power in the country. Over the last five years, this has prompted an increasing tempo of sanctions against regime officials by the US, EU, UK, and Canada. The pace of action picked up further still in November 2021 after Ortega won what was widely seen to be a rigged presidential election which allowed him to stay in office for a fourth consecutive term. In response, President Biden signed the Reinforcing Nicaragua's Adherence to Conditions for Electoral Reform Act, which enabled further sanctions against the regime.

The US subsequently applied new sanctions on regime officials and a Nicaraguan mining company in January and June 2022, and in October, President Biden signed a new Executive Order that targeted the gold sector of the Nicaraguan economy and designated the Nicaraguan national mining authority. In light of Ortega's apparent unwillingness to reform - reflected in further rigged municipal elections in November 2022, as well as Ortega's public support for the Russian invasion of Ukraine - 2023 looks likely to be a year in which sanctions are tightened further.

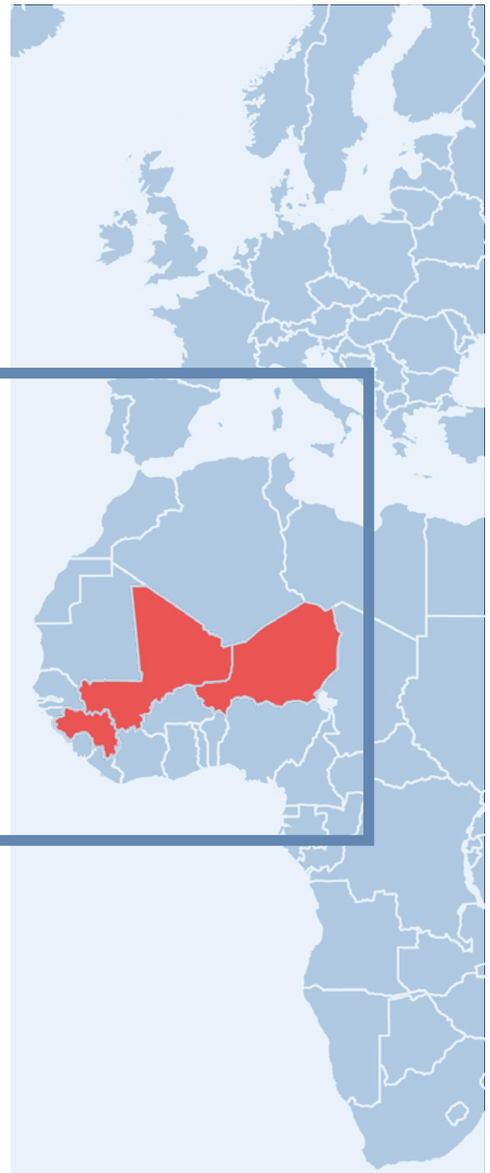
One area with the potential for a change, however, is Venezuela. Under leftist leader Hugo Chavez and his successor Nicolás Maduro, who took power in 2013, the country has been a major opponent of US influence in Latin America. The US first implemented sanctions against Venezuela in 2006, citing Chavez's lack of cooperation on terrorism and drugs trafficking, and later expanded its range of concerns to human rights and civil rights abuses from 2014 onwards, designating state officials, including Maduro and close associates, limiting financial transactions, and placing controls on the oil and gold trade with Venezuela, two of the country's major economic sectors. In 2017, the EU and Canada imposed their own sanctions on Venezuela in response to alleged human rights abuses, with the UK adding measures in 2020. In 2021, the standoff between the US and its allies and Venezuela continued, but in 2022, there have been indications of a slight thawing of relations based on Maduro's reported willingness to talk to his domestic opponents in return for some US sanctions relief.

According to reports, an easing of US sanctions would allow Chevron, a major US oil firm, to engage with the Venezuelan state-owned oil company, PDVSA, but not to drill or export any petroleum of Venezuelan origin. 2023 might see some very limited loosening of at least US sanctions on Venezuela, although President Biden will face severe domestic criticism from the Republican Party if he does so.

A further development of note in Latin America was OFAC's designation in November of two individuals, Russian and Belarusian nationals, and their businesses, for using bribery to influence business in **Guatemala's** mining sector. As with the Moldovan example above, the designations indicated that the US would seek to identify malign Russian influence globally as an adjunct to its sanctions campaign against the invasion of Ukraine.

Africa

With western eyes focused on events in Europe and Asia in 2022, new sanctions measures in Africa have been relatively limited. In the wake of a military takeover of Sudan in October 2021, international institutions and western countries suspended aid to the country, and in March 2022, the US imposed sanctions on Sudan's Central Reserve Police for the brutal treatment of civilians protesting against the coup. Other US actions included the designation in August of three politicians in **Liberia** for their ongoing involvement in corruption.



2022 has witnessed African states using sanctions themselves as a form of influence, especially for promoting democracy, with ECOWAS the prime mover.

However, 2022 has witnessed African states using sanctions themselves as a form of influence, especially for promoting democracy, with the Economic Community of West African States (ECOWAS) the prime mover. 2021 ended with ECOWAS threatening to impose sanctions on the military regime in **Mali** if it failed to hold democratic elections in early 2022, a threat that was fulfilled with a full financial and trade embargo in January 2022, when the regime reneged on previous commitments. In a rare example of sanctions having their desired impact at speed, ECOWAS lifted the sanctions in July after the Malian military agreed to a transition to democracy over two years, underpinned by a new election law.

In September 2022, ECOWAS applied economic statecraft again, announcing more limited sanctions against the military regime in Guinea due again to a failure to move towards democracy. Following a military coup in **Burkina Faso** in September (the second of the year), ECOWAS encouraged the military regime in Ouagadougou to plan for a return to democracy. Still, with progress looking uncertain, there is potential for further measures against it by the West African group in 2023.

Thematic Review

Both democratic and authoritarian countries have long used UNSC sanctions as a means of tackling shared international challenges such as humanitarian crises and threats from organized crime, terrorism, and weapons proliferation. However, as noted above in the discussion of North Korea, UNSC activity in these areas has slowed significantly in recent years, as any agreement between the permanent members has become more difficult to achieve. One example of collaboration in 2022 was the agreement on a set of sanctions on Haiti in October, imposing an arms embargo and designating individuals responsible for undermining peace and stability on the island. However, this was a rarity, and as a result, most thematically targeted sanctions in 2022 were imposed by autonomous national regimes - in particular, those of the US, EU, Canada, UK, and Australia.

Crime

The US has used 2022 to target **organized crime** - a stated strategic aim highlighted in December 2021 with President Biden's creation of a United States Council on Transnational Organized Crime (USCTOC). Drug trafficking has been a particular priority. In April, OFAC designated the Kinahan Organized Crime Group (KOCG), an Irish gang responsible for importing illegal narcotics from Latin America into Europe, along with seven of its key members, while in July, OFAC targeted Obed Christian Sepulveda Portillo, a weapons trafficker for the Mexican group, Cartel de Jalisco Nueva Generacion (CJNG). In addition, the US focused on the Illegal Wildlife Trade (IWT), designating Malaysian national Teo Boon Ching and his network in October for the smuggling of rhino horn, ivory, and pangolins from Africa to East and Southeast Asia.

As noted above in several national updates, the US also applied sanctions in 2022 to target cybercrime, as well as pursuing those they deemed to be cybercrime enablers, especially in the provision of cryptocurrency services. The targeting of cryptocurrency mixers Blender and Tornado Cash were major firsts, and although the designations were linked primarily to North Korean activity, OFAC noted the role that both platforms played in support of online criminality more generally. These mixing platforms were not alone, moreover, and there were a number of other significant cybercrime designations.

In April, OFAC sanctioned Hydra Market, a Russia-based darknet market for illegal products and services in tandem with cryptocurrency exchange Garantex, which it alleged was an exchange of choice for cybercriminals seeking to launder funds from ransomware attacks. There were signs, too, that OFAC was pursuing US-based firms for potential sanctions failures, with the announcement of a $24 million settlement fine with Seattle-based cryptocurrency exchange Bittrex in October, relating to transactions of over $250 million, which violated Iranian and other US sanctions. In August, press reports also alleged that OFAC was investigating the major cryptocurrency exchange Kraken for similar violations.

However, OFAC's pursuit of cybercrime and sanctions evasion enablers in the cryptocurrency sector has led to some difficulties, with some in the industry arguing that the US was going too far in designating entire platforms with no evidence of complicity in criminality. In the case of Tornado Cash, for example, an industry outcry about its designation also potentially sanctioning the open-source code used to create the platform led OFAC to revise its advice in September to clarify that it did not do so. In the same month, it was also revealed that Coinbase, a major exchange, was financially supporting a lawsuit filed against OFAC by six of its employees who had been users of Tornado Cash, arguing that OFAC should be targeting bad actors misusing platforms rather than the platforms and the majority of innocent users. However, OFAC is unlikely to be dissuaded from focusing ever more intensely on the sector, even if the industry wins some individual battles over platform designations.

Terrorism

In addition to crime, the US has been active in the use of sanctions against **Islamist extremist** terrorism. In March, OFAC designated a UAE-based financing cell linked to the Nigeria-based terrorist group Boko Haram, and in May, a financing network of individuals and companies operating across the Middle East and North Africa, which had raised over $500 million for the Palestinian group, Hamas. Later in the year, OFAC shifted focus to East Africa, designating facilitators and weapons traffickers for al-Shabaab in October, and made its first designations against the Islamic State (IS) affiliate IS in Somalia in November. One of the points of interest in these designations has been the focus on undermining the terrorist financing of groups as a way to continue to limit their operational effectiveness, and similar designations will probably continue in 2023.

One area of innovation in terrorist designations that will probably develop further in 2023 will be the targeting of extreme right groups, potentially linked to the support for the conflict in Ukraine. In October, for example, OFAC sanctioned the neo-Nazi group Task Force Rusich for raising funds to support fighters on the Russian side in Ukraine. Extreme right-wing fundraising is a major concern in the crowdfunding sector, as well as for cryptocurrency platforms and fiat payment service providers. With the growth of the extreme right, a concern for FATF and national governments - inflamed this year by the war in Ukraine - further designations and some enforcement actions against firms that have failed to undertake adequate due diligence are probable in 2023.

Human Rights and Corruption

A final area of activity in 2022 fell under the banner of 'Global Magnitsky' style sanctions, which target perpetrators of human rights style abuses, and in some national regimes, corruption. As noted previously, the US led the way in creating a Global Magnitsky regime in 2016, but since then has been followed by Canada (2017), the EU (2020), the UK, and, in December 2021, Australia. In 2022, the US applied Global Magnitsky legislation in several 'niche' cases, such as its designations of the Sudanese police and corrupt Liberian politicians mentioned above, but also as a way of sending a broader political message linked to wider geopolitical concerns, as in the cases of designated Russian corruption in Moldova and Guatemala.

Australia took a similar approach, making the first use of its own Global Magnitsky legislation in March 2022 in the wake of the invasion of Ukraine, targeting 14 Russians linked to corruption and 25 "perpetrators and accomplices" connected to the death of Magnitsky himself. In the same month, the US also used its Magnitsky law to sanction further Russian officials linked specifically to Magnitsky's persecution.

Overall, however, 2022 was a relatively limited year for applying Global Magnitsky sanctions, with designation activity heavily focused on large strategic concerns such as the invasion of Ukraine and weapons proliferation. This seems disconcerting to their supporters, especially given the level of effort made by civil society groups to encourage their adoption by western countries in recent years. However, they will undoubtedly remain a valuable tool in the democratic community's armory both for individual cases and - in some instances - as elements within wider packages of measures directed at larger targets. As and when geopolitical crises abate, they are likely to come back to the forefront of attention and usage.

What does this mean for your firm?

"Despite governments' focus on major international crises, firms should also continue to pay close attention to wider regional and thematic developments in applying sanctions. One area where particular work will be needed is in identifying potential exposure to Russian sanctions evasion, even in regions far from the war in eastern Europe. In addition, the intensifying US interest in the abuse of cryptocurrency should encourage CASPs to urgently assess their potential exposure to sanctions risks and review whether they require better data and technology in place to mitigate them."

Alia Mahmud
Regulatory Affairs Practice Lead, ComplyAdvantage

Sanctions Trends for 2023

The failure of the UNSC to take action on Myanmar or North Korea indicates that while there are significant geopolitical divisions between western countries and authoritarian powers, it will cease to be a forum for agreeing on collective international action on major issues. The illegal invasion of a sovereign state by one of its permanent members in February 2022, opposed by three of the other permanent members but tacitly condoned by the fifth, suggests that this situation will remain for some time.

The Western Front

This will further encourage the existing trend towards applying national autonomous regimes, especially by western governments. The US will remain at the forefront of this, underpinned by its strategic review in October 2021 that emphasized sanctions' role as a major tool of US foreign policy, supporting national security interests, promoting democracy, combatting authoritarianism, and targeting corruption and human rights and civil liberties. The review also highlighted the importance of targeting new technologies and crypto assets and traditional fiat systems, trade, and commerce, a direction that has been evident in 2022.

In 2023, the US will continue to apply sanctions along similar lines, although domestic political pressures are likely to impact how President Biden proceeds following the Republicans' narrow victory in the House of Representatives in November 2022. The Trump administration was an even more active applicant of sanctions. Many Republicans would like to see them used more aggressively against China and Iran and are uncomfortable with the thought of relaxing measures against Iran or other opponents, such as the Maduro regime in Venezuela. With a presidential election coming in November 2024, neither the Democrats or Republicans will wish to appear 'soft' on perceived enemies.

Alongside the US, European, Anglophone, and Asian countries such as Japan which have their own regimes, will use them more widely, and where there are key shared issues, will seek to both coordinate and consolidate their approaches. As noted earlier, one effect of the Russian invasion of Ukraine has been to engender a step-change in cooperation between several democratic powers, with countries not only seeking to act in partnership but also 'catch up' with existing sanctions already put in place in previous years by the US. This is likely to continue in 2023, with greater consistency over Iran, for example. There will also be more efforts to coordinate measures on sanctions implementation and effectiveness, such as the REPO group. However, with so many legal practicalities to work through at domestic levels on fundamental issues like 'Freeze to Seize,' it is unlikely that these initiatives will have anything other than a marginal effect in the short term. If resolved, however, they offer the prospect of a more powerful combined western sanctions' front' in the future.

The real test of this growing western unity on sanctions in the short to medium term will be their use against China in the event of a crisis over Taiwan. How each country will react is not predictable, and much would depend on the specific contours of the crisis if it emerges. An invasion will not threaten the physical security of the EU, UK, and Canada, and none have a security relationship with Taiwan comparable to that of the US. Given the centrality of China to the global economy, they are likely to be more circumspect than the US or countries in Asia-Pacific about aggressive sanctions before the use of force by China. However, if China were to invade, it's more likely than not that western countries would deliver a similarly coordinated response to what has been seen with Russia.

Unintended Consequences

In the medium to long term, however, it is important to note that there are other issues that will create challenges for the west's increasing reliance on sanctions - issues that will become more obvious the more sanctions are used. Policymakers and researchers are debating once again how effective sanctions are in achieving their goal of behavioral change, as opposed to acting as purely punitive measures (see, for instance, Agathe Demarais's 2022 book, 'Backfire: How Sanctions Reshape the World Against US Interests').

Limited implementation in less well-resourced jurisdictions, gaps in coverage of key sectors, and the rejection of western sanctions by many non-western states, combined with sophisticated sanctions evasion techniques, have allowed targeted countries to survive - if not thrive - in the face of tough sanctions regimes. This theory holds especially well in countries with authoritarian governments with the power to suppress unrest. Indeed, where the leaderships of those countries are not overly concerned about the economic hardship of their own people, sanctions are unlikely to have a direct impact on decision-making unless they prohibit the regime from accomplishing high-priority goals (such as developing WMD or ballistic missile technology) or put the regime in danger.

A further concern is humanitarian consequences. Sanctions, however tightly targeted, contribute to increased poverty, especially in developing countries. In a study published in 2022, the European Council on Foreign Relations found that sanctions on Iran had triggered high inflation, making common household goods unaffordable to most of the populace. Sanctions can also have other unwanted economic consequences. In a statement in July, the UN Special Rapporteur on Unilateral Coercive Measures raised concerns about the effects of over-compliance with unilateral sanctions by financial institutions, increasing the financial and economic exclusion of many vulnerable people. Such externalities are likely to become more obvious to western countries over time, especially if they lead to more economic hardships within western countries, too, as might well be the case as the result of rising gas prices following sanctions against Russia.

An Authoritarian Coalition?

A further final anxiety around sanctions is their long-term effect on the relationships between targeted states and the impact on the global power balance between democracies and authoritarianism. Some targeted states - Russia, Iran, North Korea, and Venezuela, for example - have shown signs of increasing political and economic collaboration in the face of western hostility, including cooperation on sanctions evasion, and as noted before, Russia and China have become blocks on international action via the UN. These developments have led to fears in some quarters of a so-called 'authoritarian axis' emerging, with the potential for a new economic and financial order anchored around the Chinese economy acting as a separate counter-weight to the current US dollar-dominated financial system.

For example, the war in Ukraine has led to increased use of the Chinese yuan in Russia, with trading on the Moscow Exchange rising from 0.5 percent of transactions in January to 26 percent in August and several large Russian companies issuing yuan-denominated bonds. If such a situation were to develop further, then - ironically - western sanctions dependent for their impact on the widespread use of the US dollar would lose their effectiveness.

At present, however, such fears are probably overblown. China has made little use as yet of its own regime in response to western measures and has maintained a careful position concerning western sanctions on Russia, largely following their requirements while refusing to endorse their usage publicly. Unless western countries applied similar measures against China in the event of an invasion of Taiwan, China seems unlikely to throw in its lot with Russia and others on developing an alternative financial system for the present, and without China, any authoritarian axis would lack economic potential. Nonetheless, western countries should recognize the potential long-term economic and financial consequences of authoritarian regimes feeling driven to work together.

What does this mean for your firm?

"Firms should expect western governments to follow the trend of the last decade and continue to apply sanctions as a primary tool of policy in the international arena. Over time, they should also expect national autonomous regimes in Canada, the UK, the EU, and elsewhere to show greater consistency, consolidation, and coordination with that of the US. In terms of crisis, therefore, they should be prepared for significant volleys of new designations."

Alia Mahmud
Regulatory Affairs Practice Lead, ComplyAdvantage

← Previous section

Next section →

Regional Regulatory Trends

When asked which area of the compliance function would be at risk in an audit,

48%

- the highest proportion - told us it would be their knowledge of regulations. So in this section, we explore the evolving anti-money laundering regulatory landscape, examining global trends and key themes in major economies. It provides a breakdown of significant new and proposed legislation as well as how firms should prepare for this in 2023.

Priorities for FATF Singaporean Presidency (2022 – 2024)

Singapore took over the FATF Presidency on July 1, 2022, establishing the global AML/CFT standard setter's priorities for the next two years. These include:

- **Strengthening asset recovery** - As less than one percent of illicit assets are recovered, FATF will seek to enhance collaborative frameworks and focus on cyber-enabled crimes such as fraud, scams, and ransomware using data analytics and enhanced work through public-private partnerships. The first FATF-INTERPOL Roundtable Engagement (FIRE) was held in Singapore in September.
- **Countering illicit finance associated with cyber-enabled crime** - A new initiative will look to understand the money laundering and terrorist financing related to online fraud, ransomware, phishing attacks & scams and document best practices.
- **Increasing the effectiveness of global AML measures** - The FATF will organize thematic sharing sessions and focus on identifying new ML/TF risks linked to VASPs and sharing best practices, completing guidance on the beneficial ownership of legal persons, and amending FATF regulation 25 on beneficial ownership of trusts and legal arrangements by February 2023. It will also encourage the adoption of data analytics for better AML/CFT outcomes and work to develop a regular review of TF risks with Al Qaeda, ISIL & affiliates. Finally, it will aim to generate awareness of the ML/TF risks related to environmental crime, the international wildlife trade, and grand corruption
- **Reinforcing FATF Partnerships with FATF-style regional bodies (FSRBs)** – The FATF will look to build capabilities and capacity to strengthen the Global Network to more effectively tackle money laundering, terrorist financing & proliferation financing.

The FATF also recently published a report on Illicit Proceeds Generated from the Fentanyl and Related Synthetic Opioids Supply Chains. The report was commissioned following increased overdoses reported in North America, Africa, and Asia linked to recreational and other non-medical use of fentanyl and opioids. It contains risk indicators to help financial institutions and regulated firms identify suspicious activity and detect and disrupt money laundering linked to the drug trade.

Russia and Higher Risk Countries and Jurisdictions

The FATF suspended Russia's involvement in its activity due to violations of its core principles to "promote [the] security, safety and the integrity of the financial system." This followed statements from the FATF in March, April, and June condemning Russia's invasion of Ukraine. Russia cannot participate in FATF project teams, peer-review processes, meetings of FSRBs as a member of FATF, hold leadership or advisory roles, or be part of the decision-making process in the FATF.

The FATF also added the DRC, Mozambique, and Tanzania to its grey list and removed Nicaragua and Pakistan at its plenary in November 2022. Myanmar was added to the blacklist, which includes Iran and North Korea.

Upcoming Mutual Evaluations

The FATF has indicated that it will set the groundwork for the fifth round of mutual evaluations, increasing frequency, making them more targeted around key risks, applying greater scrutiny, and emphasizing increasing effectiveness.

It is anticipated that the following countries' Mutual Evaluations will be discussed at plenaries held next year: Algeria, Angola, Belize, Brazil, Brunei, BVI, Comoros, El Salvador, Guyana, Indonesia, Iraq, Lao, Lebanon, Lesotho, Luxembourg, Macedonia, Nepal, Kenya, Palestine, Qatar, Romania, Sao Tome & Principe, Sudan.

This may lead to additional countries being added to, or removed from, the grey list. Mutual evaluation reports reviewed or adopted in 2022 for the following countries are likely to lead to an array of legislative activity in 2023 to address shortcomings identified by the FATF: Anguilla, Bolivia, Chad, Curacao, Ecuador, Gabon, Germany, Guinea, Kazakhstan, Kenya, Liberia, the Netherlands, South Africa, and Venezuela. The FATF has a full calendar of activities available on its website.

What does this mean for your firm?

"Firms should review any papers and studies issued by the FATF to ensure that they remain abreast of key risks and emerging trends and can update their internal systems and controls with guidance and typologies that apply to their operating environments. Firms should also ensure that their policies remain up-to-date, listing higher-risk countries and jurisdictions to identify higher-risk customers and transactions to apply enhanced due diligence. If there is a flurry of activity around Russia, firms should remain vigilant to indirect exposure to transactions that could finance the invasion of Ukraine."

Alia Mahmud
Regulatory Affairs Practice Lead, ComplyAdvantage

North America

United States

Under the Biden administration, the US will continue focusing on three core themes:

01.

Strengthening laws and regulations to tackle illicit financial flows

02.

Modernizing, building, and enhancing regulatory and enforcement frameworks, particularly in the crypto space

03.

Targeting wrongdoers who seek access to the US financial system to launder the proceeds of crime

National Illicit Finance Strategy 2022

The US published its 2022 National Illicit Finance Strategy, providing a roadmap to "close loopholes exploited by criminals and illicit actors." This is designed to address threats and vulnerabilities identified in its National Risk Assessment (NRA) that have resulted from increased levels of fraud, corruption, and the digitization of finance. Particular emphasis was placed on addressing Russian aggression in Ukraine and the global network of corrupt Russian elites.

The strategy set four priority recommendations with 14 supporting actions.

Priority One:

This entails closing gaps in the AML/CFT framework that are being exploited by shell and real estate companies to anonymously access the US financial system. It aims to do this by:

- Implementing the Corporate Transparency Act
- Improving access to beneficial ownership information
- Bringing transparency to real estate transactions
- Assessing the need for additional sectors to be brought into the scope of AML/CFT measures (such as payment processors, dealers in precious metals, stones, and jewels (PMSJ), and non-bank financial institutions)
- Considering updating AML/CFT requirements for VASPs.

Priority Two:

Make the AML/CFT Regulatory Framework for Financial Institutions More Efficient and Effective

The government hopes clearer guidance, information sharing, and more funding for supervisory and enforcement bodies will improve efficiency. Workstreams include:

- Potentially updating reporting requirements and thresholds
- Ensuring that AML/CFT supervisors of non-bank financial institutions are resourced appropriately
- Enhancing risk-based supervision

Priority Three:

Enhance Operational Effectiveness in Combating Illicit Finance

The Biden administration wants to make it harder for illicit actors to find a safe haven in the US by enhancing the operational effectiveness of government agencies, international partnerships, and law enforcement. Actions include more frequent updates and communication around illicit finance risks and AML/CFT priorities, prioritizing inter-agency coordination, expanding and enhancing information sharing across public-private sectors, and strengthening the implementation of the FATF's AML/CFT standards.

Priority Four:

Support Technological Innovation and Harness Technology to Mitigate Illicit Finance Risks

With priority four, the US looks to harness technology to enable digital innovation while managing risks associated with "new" financial services, products, and activities, including virtual assets. The US will encourage the use of technology by the private sector to improve compliance and increase the use of AI and data analytics to combat illicit finance by government bodies. It will also look to make the US a leader in financial and payment technology. According to the 2024' benchmarks for progress' associated with this priority, firms can expect incentivization from the Treasury regarding the testing and use of AI for transaction monitoring within the next two years.

Each priority recommendation includes progress benchmarks that firms should familiarize themselves with.

ENABLERS Act & NDAA

The Establishing New Authorities for Businesses Laundering and Enabling Risks to Security (ENABLERS) Act was introduced to bring gatekeeper professions into the scope of AML/CFT laws and regulations. The initial draft of the act included references to lawyers, accountants, investment advisors, dealers in art and antiquities, trust and company service providers, third-party payment providers, and public relations firms that "provide another person with anonymity or deniability." Although the ENABLERS Act was included in an initial draft of the 2023 National Defense Authorization Act (NDAA) for the 2023 Fiscal Year, it was cut from the final NDAA. The ENABLERS Act has received significant support from anti-corruption groups and the Biden administration and is expected to renew its push on this legislation in 2023.

Although the National Defense Authorization Act for Fiscal Year 2023 did not include a reference to the ENABLERS Act, it did include a list of countries identified as adversaries. This includes China, Russia, Iran, Afghanistan, North Korea, foreign terrorist organizations, and ISIS in Iraq and Syria.

FinCEN and the Anti-Money Laundering Act 2020

In December 2022, FinCEN issued a Notice of Proposed Rulemaking on Beneficial Ownership Information Access and Safeguards and Use of FinCEN Identifiers for Entities. This shows how firms defined as "authorized recipients" can access beneficial ownership information (BOI) reported to FinCEN. FinCEN also proposes regulations to detail when and how companies can report beneficial ownership information using FinCEN identifiers. At the moment, only the following categories of persons would access the non-public database:

- Federal, State, local, and Tribal officials, certain foreign officials acting through a Federal agency, and intelligence and law enforcement may be able to obtain BOI for national security purposes
- Financial institutions (FIs) can access the registry for customer due diligence
- Regulators will have access to assess compliance with CDD measures

By January 1, 2023, the US Government must review new beneficial ownership reporting requirements.

Crypto Regulatory Framework

Significant progress has been made toward developing a national crypto regulatory framework. However, much uncertainty remains over the final shape this will take.

The Digital Asset Development Framework

The Digital Asset Development Framework was launched to create "a clear framework for responsible digital asset development and pave the way for further action at home and abroad." This followed President Biden's Executive Order on Ensuring Responsible Development of Digital Assets, which set out the first whole-of-government approach to mitigating risks while channeling the benefits of digital assets and technology.

The framework includes recommendations on:

- Protecting consumers, investors, and businesses
- Promoting financial stability
- Countering illicit finance
- Reinforcing US financial leadership and economic competitiveness
- Promoting financial inclusion
- Advancing responsible innovation
- Exploring a US central bank digital currency (CBDC)

The framework sets the timelines for activities to be carried out by the US Treasury. This includes completing an illicit finance risk assessment on decentralized finance by February 2023 and evaluating non-fungible tokens (NFTs) by July 2023.

The Treasury will also work to determine whether to amend the Bank Secrecy Act (BSA), anti-top-off statutes, and laws on unlicensed money transmitters to cover digital asset service providers. Further consideration will be given to increase penalties for unlicensed money transmitting and to give powers to the Department of Justice to take legal action in any country where there is a victim of digital asset-related crimes. The Federal Reserve is also expected to launch FedNow to carry out interbank clearing 24/7 and support instant payments.

The US will also look to expand its leadership role in the digital assets space by working within international organizations and standard-setting bodies, such as the G7, G20, and the Financial Action Task Force (FATF). The Biden administration has already developed policy objectives for a US CBDC system.

The Lummis-Gillibrand Bill

The Responsible Financial Innovation Act - commonly known as the Lummis-Gillibrand Bill - was introduced to develop a regulatory framework for crypto at the federal level. If passed, the act will define digital assets and clarify which authority is responsible for what. It will also create a regulatory structure for stablecoins and a regulatory sandbox for responsible firms.

Digital Assets Anti-Money Laundering Bill

Two US Senators introduced a Digital Assets Anti-Money Laundering Bill in late December. The bill introduces several provisions. First, it aims to extend customer due diligence obligations to wallet providers, ATM providers, and miners. It also calls for the SEC to establish a risk-focused examination and review process and prevent financial institutions from dealing with mixers, privacy coins, or anonymity-enhancing technology. It further calls on FinCEN to classify money service businesses (MSBs) as "custodial and unhosted wallet providers, cryptocurrency miners, validators, or other nodes who may act to validate or secure third-party transactions, independent network participants, including MEV searchers, and other validators with control over network protocols [sic]."

NYDFS Guidance for Banks

In December 2022, the New York State Department of Financial Services (NYDFS) issued an industry letter guiding state-regulated banks on getting prior approval for virtual currency-related activity. This letter was designed to act as a reminder that there is an expectation that they must obtain approval from DFS before offering virtual currency-related services. Obliged entities must send a written document to the NYDFS that covers their business plan with a description of the proposed crypto activity, an overview of enterprise risk management policies, corporate governance and oversight arrangements, consumer protection provisions, financials, and legal and regulatory analysis.

Criminal Proceedings

The United States Department of Justice will continue to issue fines and work with international partners to protect the U.S. financial system against illicit finance. In December 2022, Denmark's Danske Bank agreed to forfeit $2 billion after pleading guilty to defrauding U.S. banks by failing to disclose deficiencies in its AML/CFT systems and controls. Danske Bank Estonia also failed to disclose the high-risk profile of non-resident customers, including those from Russia, which led to the largest money laundering scheme in recent times. The Securities and Exchange Commission (SEC) also issued a settlement with Danske Bank for $413 million, including a civil penalty of $178.6 million.

In December 2022, the US Department of Justice issued an indictment against FTX Founder Samuel Bankman-Fried and worked with partners in Bermuda to secure his arrest and extradition. Charges include conspiracy to commit wire, commodities, and securities fraud, wire fraud, conspiracy to commit money laundering, and conspiracy to defraud the Federal Election Commission and violate campaign finance rules. This follows the collapse of FTX, leading to the loss of billions of consumers' dollars through "misappropriation of the customer deposits to pay expenses and debts of a different company he also owned as well as make other investments." The case will continue into 2023 and is already spurring a flurry of legal and regulatory activity worldwide.

Canada

Canada will continue to boost its anti-money laundering defenses and capacity to fight financial crime. This includes fast-tracking the implementation of a publicly accessible corporate beneficial ownership registry before the end of 2023. The government further signaled that it would establish a new Canada Financial Crimes Agency to enhance the country's ability to respond to complex and fast-moving financial crime cases.

Grappling with changes to Canada's AML/ATF Laws

Several legislative changes were introduced in the AML and anti-terrorist financing (ATF) space after the Canadian government issued a public order under the Emergencies Act to end the occupation of Ottawa by Canadian truckers in Covid-19 protests. The government extended AML/ATF requirements to crowdfunding platforms and payment service providers (PSPs) who held property for - or had customers suspected of - supporting the illegal blockade as customers.

This led to the amendment of the following pieces of legislation:

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR)
- Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties (PCMLTFAMP) Regulations

Changes included updating the definition of electronic funds transfers, bringing crowdfunding platforms fully into the scope of AML/ATF requirements, and certain payment service providers previously carved out by PI-7670 guidance now covered as money services businesses (MSBs) or foreign money services businesses (FMSBs).

Credit, debit, and prepaid payment product funds transfers are now considered electronic fund transfers (EFTs), and foreign and domestic money services businesses (MSBs) now have additional obligations related to EFTs. FINTRAC updated its MSB registration guidance and developed a tool to help MSBs identify if they need to register with the regulator. MSBs will continue to navigate these changes into 2023, set up AML/CFT compliance programs, and prepare for the supervision of these newly covered activities.

FINTRAC

In its annual budget, the Government of Canada allocated $89.9 million to FINTRAC over five years to allow it to explore how to adopt innovative, technology-based solutions and enhance private sector engagement. FINTRAC will continue to focus on combating online child sexual exploitation, money laundering in British Columbia, the trafficking of illicit fentanyl, romance fraud, and human trafficking in the sex trade.

It is also anticipated that FINTRAC will carry out a strategic review of changes introduced in June 2021 to comply with updated FATF standards. This is expected to lead to the implementation of the travel rule requiring originator and beneficiary information for transfers over $1,000 in virtual currencies and new AML/ATF requirements for prepaid credit cards and other prepaid products. FINTRAC also published an operational alert containing terrorist activity financing indicators at the end of December.

Review of AML/ATF Regime

The Canadian government has indicated that it will conduct a comprehensive review of the AML/ATF regime, partially informed by the Cullen Commission's report. This is likely to lead to legislative proposals to close identified gaps and bolster the ability of authorities to detect, deter, investigate, and prosecute financial crimes.

Released on June 15, 2022, the Cullen Commission's inquiry into money laundering in British Columbia argued that Canada's federal anti-money laundering regime is "not effective" and featured several recommendations.

These include the appointment of an independent AML commissioner with strategic oversight of responses to money laundering at the provincial level, requirements to report on new legislation regularly, and ensuring that money laundering has more attention and increased monitoring.

The Cullen Commission further recommended regulating MSBs, which are currently subject to oversight by FINTRAC under the PCMLTFA, at the provincial level. There are also calls to mitigate trade-based money laundering by creating a Trade Transparency Unit to identify anomalies in Canadian trade data and "detect and measure the flow of illicit funds without needing to examine every shipment of goods into and out of the country."

It is also anticipated that a financial sector legislative review will focus on digitizing money and maintaining financial sector stability and security. The first phase will focus on digital currencies, including crypto and stablecoins.

Fines

Canada has issued an increasing number of fines for PCMLTFA violations, and this trend is likely to continue. FINTRAC fined the Laurentian Bank of Canada CAD$486,750 for its failure to submit suspicious transaction reports when it had reasonable grounds to suspect money laundering was taking place. This is Canada's second-largest penalty to date. It has also issued fines against credit unions, real estate brokers, MSBs, and one dealer in precious metals.

In its annual budget, the Government of Canada allocated $89.9 million to FINTRAC over five years to allow it to explore how to adopt innovative, technology-based solutions and enhance private sector engagement.

Europe

The European Union

AML Package

Progress will continue with the overhaul of the EU's AML/CFT regulations as the AML package moves through the EU governance process. The proposal was launched in 2021 and consisted of four separate pieces of legislation, including:

- Regulation to establish a supranational Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)
- A new AML/CFT Directive, the "new" 6AMLD for countries to implement domestic AML/CFT frameworks
- Regulation establishing a single AML/CFT rulebook with greater clarity and guidance for firms required to meet AML/CFT obligations ('obliged entities')
- Updated transfer of funds regulation to cover changes to processing transaction requirements and bring into scope virtual assets service providers (VASPs)/crypto asset service providers (CASPs)

In June 2022, an agreement was reached on creating the AMLA and giving it direct supervisory powers over higher-risk and systemically important credit and financial institutions and crypto asset service providers. A provisional agreement was also reached on updating rules on transferring funds information to comply with travel rule requirements for crypto assets.

In December, the European Council agreed to close potential AML loopholes by launching the new rulebook and "new" 6AMLD. This includes extending AML/CFT rules to crypto asset service providers (CASPs) to carry out CDD on customers and when carrying out a transaction of EUR1,000 or more, plus additional risk mitigation measures for transactions in self-hosted wallets.

Additional industries to be brought into scope include third-party financing intermediaries, traders in precious metals, stones, and cultural goods, and jewelers, horologists, and goldsmiths. An EU-wide cash payments limit will be set at a maximum limit of EUR10,000, and the EU will have a "black list" and a "grey list" to transcribe FATF's list of higher-risk countries.

Rules on beneficial ownership and multi-layered ownership have also been sharpened. An additional clarification includes the need for member states to make sure that legitimate interest is demonstrated to gain access to beneficial ownership registries, and should include journalists and civil society organizations that fight financial crime.

When approved, the AML/CFT package will trigger the largest overhaul of AML/CFT regulation in European history and has been described as "a tectonic shift" in the EU's approach to fighting financial crime.

The Current State of Implementation for 5AMLD and the "old" 6 AMLD

The European Commission will continue to name countries that have not yet fully complied with the transposition of 6AMLD, which sets out predicate offenses for money laundering. In February 2022, it launched infringement proceedings against Latvia, Lithuania, Malta & Portugal for not sufficiently explaining how they have defined predicate offenses in domestic legislation. 6AMLD became effective on December 3, 2020, and needed to be implemented by regulated entities by June 3, 2021.

Other Initiatives

New Convention for Environmental Crime

The Council of Europe is set to draft a new global Convention to Protect the Environment through Criminal Law in 2023. The draft convention will define offenses, sanctions, and responsible bodies introducing substantive criminal law, introduce preventative measures, and address issues of consequence to protect the environment through criminal law. It will also tackle civil society participation and introduce monitoring mechanisms.

Addressing De-Risking

The EBA issued a public consultation on managing ML/TF risks when providing access to financial services. The guidelines address the de-risking of vulnerable customers, such as refugees or the homeless, who cannot provide traditional identity information. A section is also included to assist financial institutions in identifying how NPOs are organized and different from other customers as well as how to manage associated ML/TF risks while providing access to financial services. The consultation closes on February 6, 2023.

Rising Money Laundering Cases

Eurojust, the EU's agency for criminal justice cooperation, found that cross-border money laundering cases have doubled in the last six years, indicating a rising trend in money laundering and enforcement actions that is likely to continue. Eurojust released its first report on money laundering for authorities investigating and prosecuting cases. The agency also found that money laundering cases account for approximately 15 percent of all cases it saw between 2016 and 2021, a significant figure.

It set up 116 joint investigation teams devoted to money laundering cases, accounting for around 25 percent of all joint investigation teams. The report found that every EU member state has been involved in some way in money laundering cases it has investigated, with Italy, France, Spain, Germany, and the Netherlands most involved. Additionally, over 60 third countries have featured in cases, particularly Switzerland, the UK, the US, and Ukraine.

France

France will continue to carry out its 2021-2022 inter-ministerial AML/CFT and proliferation financing action plan to address shortcomings identified during the FATF's March 2022 mutual evaluation review. The country will need updated legislation to bring DNFBPs, including real estate agents, into the scope of AML/CFT regulations, place more focus on managing risks associated with politically exposed persons (PEPs), and enhance monitoring.

France also needs to increase non-profit organizations' awareness of terrorist financing risks to prevent their abuse for terrorist financing purposes. The FATF has also called for France to implement fit and proper tests for senior management and beneficial owners. Its efforts will be assessed against recommendations made by the FATF in June 2025.

The Senate also recently called for the introduction of an amendment on crypto regulation, which will be put to Parliament in January 2023. A bill has been approved by the Senate amending previous laws which allowed VASPs to operate in the country without a full license until 2026.

On December 9, 2022, the Autorité de contrôle prudentiel et de résolution (ACPR) published sector-specific application principles for digital asset service providers (DASPs). These principles, which focus on AML/CFT due diligence obligations, were drawn up in conjunction with Tracfin and the Treasury Directorate General.

Specific areas covered by the guidance include the identification and classification of AML/CFT risks; the development of a risk profile for each business relationship; the identification and identity verification measures; knowledge of customers; constant vigilance with the implementation by DASPs of a system for monitoring and analyzing transactions and business relationships; reporting of suspicions; internal controls; and implementation of asset freezing measures and other restrictive measures.

Germany

Germany is set to continue improving its national AML/CFT framework after the FATF identified several deficiencies during its Mutual Evaluation Review, which also led to the Head of Germany's Financial Intelligence Unit resigning in mid-December for failure to disclose a backlog in processing SARs.

Areas for improvement identified by the FATF include:

- Enhancing the FIU's ability to process SARs, including through the use of new technology
- Addressing the under-reporting of suspicious transaction reports by non-bank financial institutions and designated non-financial businesses and professions (DNFBPs)
- Increasing awareness of the risks posed by different types of money laundering techniques, including foreign predicate offenses
- Keeping a beneficial ownership transparency register that is up-to-date and fit-for-purpose

Key actions identified include:

- Making money laundering an offense separate from the predicate offenses to allow for more effective prosecution
- Improving DNFBP supervision
- Improving SAR reporting
- Being more proactive in issuing domestic sanctions listings and designations
- Enhancing financial intelligence unit (FIU) data and analysis through better tech adoption

Germany's Finance Ministry has announced it will create a new federal financial crime agency integrated with the FIU to "follow-the-money," train more experts and speed up the digitization and connection of relevant data registers needed to tackle crime effectively.

On the enforcement side, the trial of Wirecard's ex-CEO, Markus Braun, will continue into 2023. The CEO and two managers have been charged with fraud and market manipulation and face up to 15 years imprisonment. The collapse of Wirecard reverberated across Germany, forcing the Head of BaFin to resign and generating severe criticism of the country's political class. It is also alleged that Wirecard's COO, Jan Marsalek, had links to Russia's military intelligence – the GRU – which has operated in conflict zones, including Libya. There is an international arrest warrant out for Marsalek, who remains missing.

The Netherlands

The Netherlands is also expected to address deficiencies identified in its AML/CFT framework following the FATF's MER. Actions identified include requiring all obliged firms to implement targeted financial sanctions effectively, increase resources and improve risk-based supervision, ensure that the beneficial ownership registry is populated with full and accurate information, and determine whether penalties are sufficiently dissuasive for money laundering offenses.

The UK

The UK will continue to improve its AML/CFT environment with several new measures anticipated in 2023 and a new prime minister, Rishi Sunak, who is supportive of developing an enabling environment for virtual assets and fintechs.

Legislative and Regulatory Framework

A new Economic Crime and Corporate Transparency Bill (ECB2.0) has been put before Parliament and, if successful, hopes to build on changes made in the Economic Crime Act that was approved in March 2022. The act introduced several provisions, including creating a new public Register of Overseas Entities that contains overseas entities buying, selling, or leasing land in the UK. It also increases the number of individuals subject to unexplained wealth orders, including company directors and persons who own property in trusts and in offshore accounts. Finally, the act features amendments to sanctions legislation, making it easier to impose financial penalties for sanctions breaches and increasing the information-sharing powers of the Office of Financial Sanctions Implementation (OFSI).

If successful, the ECB2.0 would introduce several additional measures around corporate registry reform, limited partnerships, changes to the Register of Overseas Entities, asset recovery, crypto assets, and additional requirements and powers to prevent and detect, investigate, and regulate economic crime. It is anticipated that the ECB2.0 will address the remaining vulnerabilities currently unaddressed by the act. As the new legislation is still being debated, amendments are likely being finalized.

It is also anticipated that the UK government will publish new and separate economic crime, anti-corruption, and fraud action plans. These will set out key objectives and steps that different authorities in the UK government will take to tackle these crimes.

This includes using new technologies, working with international partners, tackling corruption and kleptocracies, and focusing on protecting the UK's financial system. Chancellor Jeremy Hunt has also announced a review into the Senior Manager's Regime as part of 30 reforms to financial services regulation as part of the so-called 'Edinburgh Reforms' to boost growth in UK financial services.

Rishi Sunak and Crypto

It is anticipated that Prime Minister Rishi Sunak will continue to support the growth of crypto and fintech in the UK. Sunak announced plans to make the UK a "global crypto hub" during his time as Chancellor by regulating stablecoins and directing the Royal Mint to launch an NFT. The UK is also expected to continue work on exploring the launch of a Central Bank Digital Currency.

While the Financial Conduct Authority (FCA) has faced criticism in some quarters for the length of time it has taken to approve new crypto licenses, this is down to many applicants not meeting AML/CFT requirements. Additional legislative requirements for the cryptoasset sector are coming.

The Financial Services and Markets Bill is expected to "harness the opportunities of innovative technologies in financial services" in a post-Brexit world and bring stablecoins and other cryptocurrencies under existing regulatory frameworks for e-money and payments. Additional ongoing projects include a Law Commission Review of Digital Assets, a Treasury Select Committee review of crypto assets, and a Crypto All Party Parliamentary Group Inquiry into crypto assets, considering legal frameworks, risks and opportunities, and the wider approach of the UK in the crypto asset space.

Asia Pacific

China

China has issued a "Three-Year Action Plan for Combating Money Laundering Violations and Crimes (2022-2024)" to clamp down on anti-money laundering, which runs from January 2022 until December 2024. The plan was drafted to "truly safeguard national security, social stability, economic development, and the interests of the people." It was issued by 11 Chinese authorities and obliged them to:

- Increase publicity and training
- Amend the Anti-Money Laundering Law and legal interpretations related to handling criminal money laundering cases
- Strengthen intelligence-led research for judgment and cases
- Improve the analysis of money laundering typologies and anti-money laundering investigations
- Boost the ability of obliged firms to prevent and control money laundering risks

China also amended its rules to strengthen the ability of firms to fight money laundering. The rules define Customer Due Diligence (CDD) requirements, including how regulated firms should store identity and trading data. The requirements were also extended to non-bank payment companies and wealth management firms.

In November 2022, the FATF issued an update on progress made by China to address identified deficiencies in its 2019 MER. China remains non-compliant with requirements around DFNBPs, including effective supervision and the need to carry out due diligence. It is also deficient in measures, including submitting suspicious activity reports, transparency, and beneficial ownership of legal arrangements.

Hong Kong

Updated Legislation

Hong Kong recently passed its Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022, which will become effective on June 1, 2023. The bill introduces a licensing regime for VASPs and a registration scheme for dealers in precious metals and stones to align Hong Kong with FATF standards. Amendments include:

- Updating Hong Kong's definition of PEPs to match the FATF definition
- Introducing a risk-based approach to CDD for former PEPs
- Clarifying guidance around the use of recognized digital identification technology systems for CDD
- Updating beneficial ownership requirements for trusts by confirming that this includes trustees

The Hong Kong Monetary Authority (HKMA) will also be consulting with the banking sector on changes made in the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) relating to correspondent banking and guidance on other "topical issues."

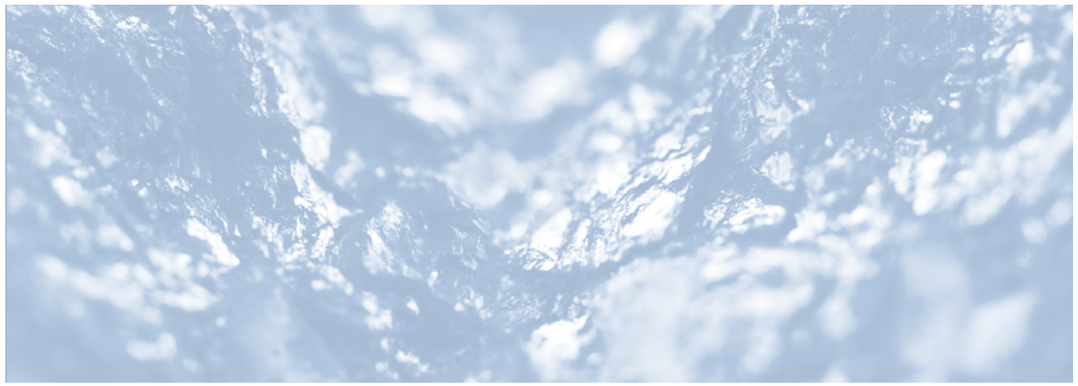
VASPs

Changes introduced by the bill are expected to create one of the most comprehensive VASP licensing regimes in the world. VASPs are defined broadly, covering payment coins, altcoins, stablecoins, and numerous governance tokens. CBDCs and financial assets already regulated by the Securities and Futures Ordinance and other non-transferable, non-fungible assets are not covered by the bill.

The proposal also grants the Secretary of Financial Services and Treasury the ability to determine which new or emerging assets are VASPs. VASPs operating in Hong Kong by March 1, 2023, must submit licensing applications by December 1, 2023, to the SFC. VASPs must have two responsible officers. Regarding penalties, VASPs operating without a license or marketing the services in HK will incur a fine of HK$5 million and a prison sentence of up to 7 years.

Dealers in Precious Metals & Stones (DPMS)

The new DPMS regime requires firms to register with the Commissioner of Customs and Excise. The two-tier registration regime orders DPMS into two groups categorized based on whether they deal in cash transactions at or above HK$120,000. The DPMS regime addresses concerns raised by the FATF in its 2018 evaluation and its recommendation that Hong Kong introduces the "appropriate level of AML/CFT requirements for the DPMS sector regarding ML/TF risks." DPMS firms have been identified as being at a higher risk of being involved in sanctions evasion, particularly in North Korea.



Singapore

Financial Services and Markets Bill

Singapore passed the Financial Services and Markets Bill in April 2022 to improve the ability of the Monetary Authority of Singapore (MAS) to address risks in the financial sector through an enhanced regulatory and enforcement framework. The sections of the bill include:

- **Harmonized and expanded powers to issue prohibition orders**, allowing MAS to ban people who are not fit and proper from holding key roles and carrying out certain activities in areas where serious misconduct has been identified or to prevent misconduct.
- **Enhanced regulation of VASPs** for ML/TF risks to align Singapore with FATF standards requiring VASPs to be licensed or registered in the jurisdiction in which they are incorporated, including those that provide digital token (DT) services outside of Singapore. A new regime was introduced to regulate these as a new class of FI and ensure that MAS has adequate oversight over these areas by creating a stronger enforcement framework and consolidating existing powers.
- **Harmonized power to impose more stringent technology risk management requirements** for for FIs or classes of FIs. It further introduces a maximum penalty of S$1 million for breaching Regulations and Notices issued by MAS.
- **Statutory Protection from Liability** for Mediators, Adjudicators, and Employees of Operators of Approved Dispute Resolution Schemes – looks to strengthen the confidence and autonomy of those resolving financial disputes and aligning the level of protection they receive with international standards.

DPT Licencing Program

Singapore will continue its work to grant Major Payment Institutions (MPIs) a license to offer Digital Payment Token (DPT) Services. As of August 2022, MAS had issued 6 DPT licenses, with Coinbase announcing it received a license in October 2022. Approximately 180 VASPs applied to the Monetary Authority of Singapore (MAS) for a license in 2020, with 17 in-principle approvals and licenses issued.

Following the collapse of Terra, Luna, and FTX, Singapore has revealed plans to make it difficult for retail investors to invest in cryptocurrencies, creating friction by potentially requiring customer suitability tests and limiting the use of credit facilities and leverage to trade in crypto. MAS has frequently issued public warnings about the risks of crypto trading and has drawn a "sharp distinction between growing an innovative and responsible digital asset ecosystem and speculation in cryptocurrency, which we actively discourage for the retail public."

In January 2022, MAS issued guidelines discouraging cryptocurrency trading by the general public and advised DT service providers to limit marketing or advertising in Singapore in public areas or via third parties.

Future Legislative Changes

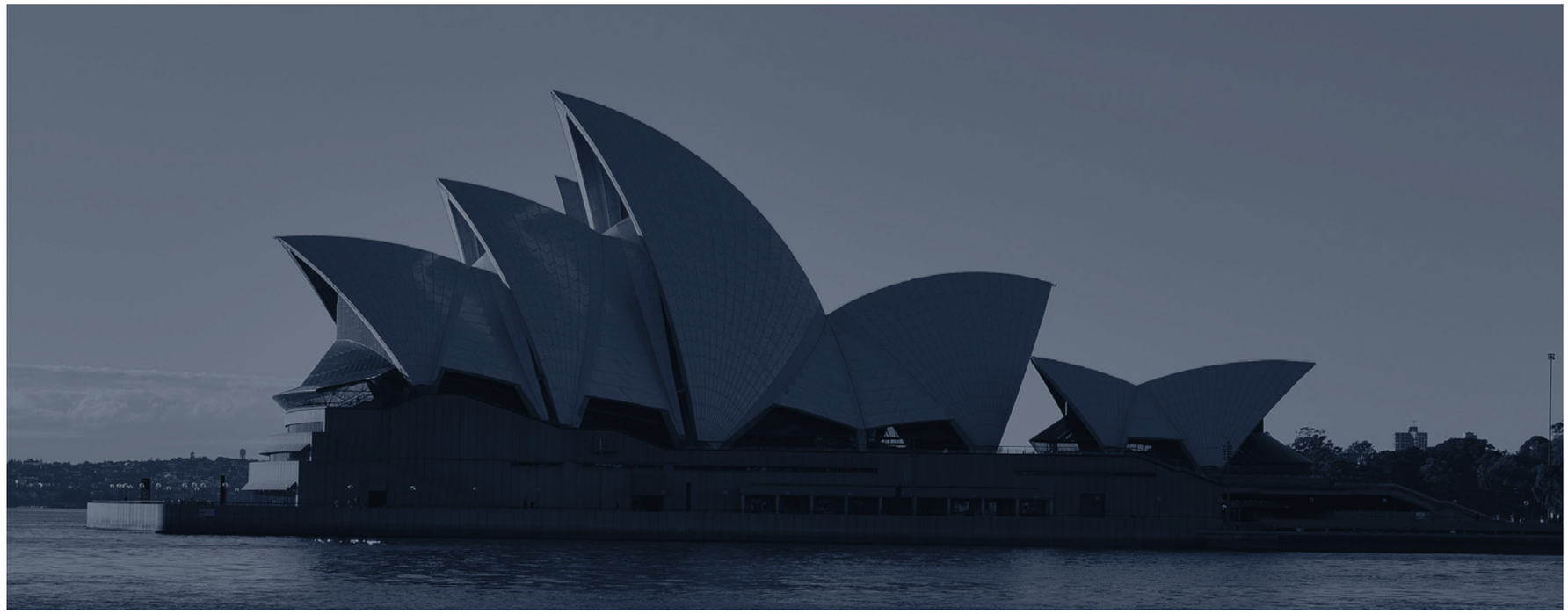
Singapore's Accounting and Corporate Regulatory Authority (ACRA) consulted on proposed amendments to the Companies Act, ACRA Act, and a new Corporate Service Providers Bill (CSP Bill), the results of which will likely be seen in 2023. ACRA's proposals look to improve Singapore's compliance with FATF recommendations, address the risks of using nominee arrangements to create shell companies for money laundering, and introduce a requirement for nominee directors to be qualified persons.

The new CSP Bill would:

- Require corporate secretarial service providers to register with ACRA as CSPs
- Increase financial penalties and introduce personal liability through a fine of up to HK$100,000 for breaching AML/CFT requirements by directors, owners, or partner of CSPs
- Introduce fit and proper training requirements for persons appointed as nominee directors by CSPs
- Create a requirement for disclosure to ACRA of nominee status and identity by nominee directors and shareholders

The amendments would also introduce a provision that CSPs' obligations will apply to proliferation financing.

Australia



DNFBPs Tranche 2 Reforms

DNFBP regulation and enforcement will continue to be a major inflection point. The Legal and Constitutional Affairs References Committee published its report in March 2022 at the request of the Senate on the effectiveness of the AML/CFT regime in Australia. The report focuses on the failure to bring DNFBPs, such as lawyers, real estate agents, casinos, and other gambling service providers, auditors, and dealers in precious metals and stones, into the scope of AML regulation.

Loopholes in Australia's AML/CFT regime have been blamed for allowing billions of dollars to be laundered through Australia's real estate sector and for "serious and systemic non-compliance" by casino operators. In 2021, out of AUS$187m in assets seized, AUS$116m accounted for real estate assets. AUSTRAC estimated that in 2020, AUS$ 1 billion was laundered by Chinese interests via Australian real estate.

The Senate report provides an overview of the regulation of gatekeepers, current and emerging challenges in AML, and various recommendations for improvement. These include regulating DNFBPs and making improvements to the AML/CFT framework, such as:

- Simplifying AML/CFT rules
- Supporting the use of technologies to meet KYC obligations
- Applying a risk-based approach to regulation
- Increasing penalties for ML/TF
- Boosting resourcing in AUSTRAC

The report further found that delays in implementing Tranche 2 reforms continue to expose Australia to economic harm and risk its credibility as it is one of only 3 FATF countries that does not have DNFBPs in the scope of AML/CFT legislation. The committee also recommended establishing a beneficial ownership registry.

Crypto Regulation

The Australian government completed its consultation on licensing and custody requirements for crypto asset secondary service providers (CASSPrs) under a planned Digital Services Act (DSA) to address regulatory gaps. CASSPrs include providers that offer crypto asset custody, storage, brokering, exchange, and dealing services or operate a market in crypto assets for retail consumers (such as peer-to-peer exchanges). The DSA is based on four key pillars:

- Technology neutrality
- Broad, flexible principles, not a prescribed code
- Regulation by an elected minister, not agencies
- Cooperation and appropriate powers, resourcing, and personnel within the government

It further calls for the taxation of crypto and the mapping of tokens. This aligns with the government's Digital Economy Strategy, which aims to make Australia a top 10 digital society and economy by 2030. This would complement the current registration regime, and AUSTRAC will continue to act as AML/CFT supervisor for CASSPrs.

AUSTRAC

AUSTRAC will continue to issue guidance to allow firms to manage ML/TF and proliferation financing risks. It released Australia's first national proliferation financing risk assessment in December. It also issued guidance to address de-risking and promote financial inclusion by providing guidance on alternative ways to verify identities. It also issued new guidance on trade-based money laundering, detecting ransomware, and preventing the abuse of digital currencies.

AUSTRAC launched enforcement proceedings against a number of firms. It started civil proceedings against Australia's largest casino operator, Crown Resorts, as well as SkyCity Adelaide and Star Entertainment Group, alleging "serious and systemic non-compliance" with AML/CFT laws. It ordered the audit of three entities under the Bell Financial Group - Gold Corporation, and Sportsbet and Bet 365 - to assess compliance with Australia's AML/CFT Act and AML/CFT rules. It also welcomed an enforceable undertaking from ING Bank Australia Group and National Australia Bank following an investigation by AUSTRAC that highlighted issues with their AML/CFT programs.

Focus on Organized Crime

Organized crime was flagged as a risk, with Australian Federal Police focusing on Italian organized crime groups (OCGs) and money laundering syndicates in the next phase of Operation Ironside.

Australian Federal Police has used the Trojan horse app AN0M to expose 51 crime groups and will look to target the 'Ndrangheta mafia, which is responsible for trafficking 70-80 percent of the world's cocaine from Calabria in southern Italy. The 'Ndrangheta mafia has been carrying out ML activities in Australian communities for decades and has a strong connection with outlaw motorcycle gangs. Law enforcement will also focus on ML that exists "only to enable global drug trafficking syndicates."

Since the launch of Operation Ironside, new laws have been passed that provide AFP with additional powers to disrupt criminal gangs. This includes the Surveillance Legislation Amendment (Identify and Disrupt) Act. It gives the AFP and the Australian Criminal Intelligence Commission (ACIC) the ability to issue three new types of warrants to collect intelligence, conduct investigations, and prosecute serious criminal activity online.

The Philippines

Since being placed on the FATF grey list in June 2021, the Philippines has taken several steps toward reforming its AML/CFT systems. As part of a FATF follow-up review in 2022, the Philippines requested a re-rating of its compliance with recommendation 28 on DNFBP supervision and regulation and recommendation 32, which covers physical currency transfers across borders.

On recommendation 28, the FATF re-rated the Philippines as largely compliant, with the country extending the 2021 Anti-Money Laundering Act (AMLA) scope to cover real estate agent developers and brokers. Gaps in the supervision of casinos were also addressed. Several minor gaps related to precious metal dealers and DNFBPs remained, however.

On recommendation 32, the Philippines was also re-rated as largely compliant. This was thanks to reforms that included domestic and foreign currency as goods under the country's Customers Modernization and Tariff Act. This clarification also strengthened the ability of enforcement bodies to demand more information from suppliers where necessary and impose fines.

Again, "minor shortcomings" remain, specifically related to the issue that truthfully declared currency cannot be seized, even when money laundering, terrorist financing, or predicate offenses are suspected.

In June 2022, the Bangko Sentral ng Pilipinas (BSP) also issued guidance for central bank-supervised financial institutions (BSFIs) on conducting institutional risk assessments (IRAs). In addition to setting out firms' regulatory obligations, the paper offers practical guidance on identifying, analyzing, and understanding the money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks that can arise from BSFI business activities and relationships.

Of the FATF's 40 recommendations, the Philippines is now rated as compliant or largely compliant with 37. Its next progress report is due on February 1st, 2023.

The Philippines has also made several strides toward crypto regulation. In July, a senior securities official revealed the country was evaluating both the EU's anti-money laundering framework and proposals issued in the US and exploring their utility for the Philippines. In December, the IMF announced it would collaborate with the BSP to create a central bank digital currency (CBDC). The IMF will provide technical support and training to the bank's staff.

Latin America

Crypto Adoption in Latin America

Crypto licensing regimes will continue to be developed in Latin America. It is estimated that the region has the highest penetration of crypto owners globally, with approximately 30 percent of people holding crypto. This is likely due to high levels of inflation in many countries, political instability, volatile currencies, and populations that are comfortable adopting Bitcoin. Argentina was the first country to issue an oil-backed digital asset, the Petro, and El Salvador was the first country in Latin America to announce Bitcoin as an official currency. In March 2022, Argentina's debt deal with the International Monetary Fund (IMF) included a statement to "discourage the use of cryptocurrencies with a view to preventing money laundering, informality, and disintermediation."

Brazil is the largest crypto market in Latin America with 10 million Brazilians trading in crypto. Its sovereign digital currency pilot was due to be operational before the end of 2022 and it has approved a regulatory framework to legalize cryptocurrency use as a payment method.

The bill defines virtual assets and creates rules for the use of crypto on a day-to-day basis. Providers are required to follow guidelines in order to safeguard personal data and client funds. It also includes penalties to address fraud. The Central Bank of Brazil will require firms that provide crypto-to-fiat exchanges, crypto custody, and crypto-related products to be licensed.

In April 2022, the Central Bank of Cuba issued a notice requiring those looking to offer crypto services to obtain a license. Applications would then be assessed based on the project's legality, characteristics, and socioeconomic interest. Licenses are valid for one year. Cuba has seen crypto become particularly popular for remittance payments.

In April, Panama also passed a bill to regulate crypto and allow the use of crypto for public and private purposes. The bill has provisions for tokenization and covers issuing digital securities, trading and using crypto assets, the tokenization of precious metals, and the use of crypto assets. Concerns remain that crypto could be used to launder money, and there are fears that the protections are not strong enough to prevent fraud. Panama has indicated that there will be effective regulation and oversight by a watchdog and that laws on financial transparency will apply to crypto transactions.

More widely, there has been a rising trend in cryptocurrency scams, with the misuse of cryptocurrencies linked to cybercrime, sanctions busting, and Colombian transnational organized criminal organizations. Few Latin American countries have introduced effective regulation and enforcement regimes for crypto.

Anti-Corruption Investigations

A spate of anti-corruption investigations has been launched against former heads of State and government. Former Mexican President Pena Nieto is under investigation for money laundering and illicit enrichment after Mexico's anti-money laundering agency, the UIF, flagged fiscal irregularities and cross-border transfers using private companies to accounts in Spain.

In Peru, official accusations have been filed against former President Pedro Castillo, alleging graft in public works contracts and acceptance of bribes and kickbacks. And Panama's former President Ricardo Martinelli is under investigation for "improperly diverting public funds" in the buy-out of a media company. This is currently being investigated as part of the "New Business" case, which alleges that Swiss, US, and Chinese banks were used to launder US$43.9 million used to make the purchase. He is also being investigated for his role in the case against the Brazilian construction company Odebrecht. This is one of the largest corruption cases in Latin America, and Martinelli's two sons were indicted in the US for laundering $28 million in bribes received from Odebrecht.

Africa and the Middle East

United Arab Emirates (UAE)

The UAE will continue to work to bring its AML/CFT regime up to scratch and seek removal from the FATF's grey list. The UAE Central Bank has released guidelines for licensed financial institutions (LFIs) to manage ML/TF risks linked to payments.

This includes requirements to develop internal systems and controls to manage money laundering risks. Firms must also carry out comprehensive enterprise-wide risk assessments on a continuous basis, conduct due diligence, and monitor transactions. Additional requirements include reporting suspicious transactions to the UAE's FIU and compliance with sanctions. The Ministry of the Economy has also called on real estate agents, gold dealers, auditors, and corporate service providers to register with their relevant AML authorities, such as the Financial Intelligence Unit (goAML) and the Committee for Commodities Subject to Import and Export Control system or face a fine for non-compliance.

The UAE has stepped up enforcement action, imposing fines exceeding Dh41 million ($11 million) in the first half of 2022.

It has also worked to assist in international cooperative efforts. In June 2022, Dubai Police arrested the Gupta brothers accused of stealing billions of dollars of public funds from South Africa.

In March 2022, the Dubai Financial Services Authority (DFSA) issued a consultation paper setting out how it would regulate cryptocurrencies. Dubai Law No. 4 of 2022 - known as 'The Virtual Asset Law' - established the Dubai Virtual Asset Regulatory Authority (VARA) for virtual currency activity carried out in onshore Dubai. The VARA has powers over:

- Regulating the issuance and release of virtual assets and NFTs
- Regulating and licensing virtual assets service providers
- Protecting the personal data of users and beneficiaries
- Regulating and monitoring the platforms offering cryptocurrencies and digital wallets
- Monitoring digital transactions
- Preventing the manipulation or modification of prices of virtual assets
- Operating and managing virtual assets platforms services
- Exchange services between virtual assets and currencies, whether national or foreign
- Exchange services between one or more forms of virtual assets
- Virtual asset transfer services
- Virtual asset custody and management services
- Services related to the virtual asset portfolio
- Services related to the offering and trading of virtual tokens

And it requires licenses to be obtained by persons provisioning:

- Virtual asset platform operation and management services
- Services for the exchange between virtual assets and national or foreign currencies
- Services for the exchange between one or more forms of virtual assets
- Virtual asset transfer services
- Virtual asset safekeeping, management, or control services
- Services related to virtual asset wallets
- Services related to offering, and trading in, virtual tokens

The DFSA also released Consultation Paper No. 143, which defines a regulatory framework for crypto tokens. It includes a definition of crypto tokens and looks to allow for a number of services to be provided for crypto tokens:

- Dealing in investments as principal
- Dealing in investments as an agent
- Arranging deals in investments
- Managing assets
- Advising on financial products
- Operating an exchange
- Providing custody
- Arranging custody
- Operating a clearing house
- Operating an alternative trading system

The UAE government also introduced Cabinet Resolution No. (24)/2022, amending provisions for laws on countering money laundering and combating the financing of terrorism and illegal organizations. It amends federal laws on AML/CFT and introduces a number of definitions and provisions for financial institutions and DNFBPs.

South Africa

South Africa adopted the General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Bill to address deficiencies identified in its FATF MER. By amending a number of major pieces of legislation, the bill looks to require the disclosure of beneficial owners, ultimate controllers of trusts, companies, and non-profit organizations (NPOs).

It also aims to address gaps identified against the majority of the FATF recommendations, with the remaining FATF recommendations addressed by The Protection of Constitutional Democracy against Terrorist and Related Activities Amendment Bill 2022, which at the time of writing is with the legislature.

This will support the need to draft a national risk assessment, improve the supervision of higher-risk sectors, enhance the investigation and prosecution of financial crime alongside asset recovery, make beneficial ownership more easily available, implement targeted financial sanctions, and deepen domestic and international cooperation.

South Africa has defined crypto assets or "a digital representation of value" as a financial product. This has allowed them to be regulated.

Authorities have indicated that they will introduce foreign exchange controls and licensing requirements for companies trading in crypto.

as well as firms providing advice or intermediary services. Regulation will look to mitigate the risk of theft and money laundering and for monetary policy to be undermined.

Crypto Regulation & Adoption

Africa

The implementation of crypto regulation across sub-Saharan Africa is minimal, with only one-quarter formally regulating crypto and two-thirds introducing some restrictions. This includes Senegal, Mali, Burkina Faso, Niger, Nigeria, Chad, Togo, Benin, Ghana, Ivory Coast, Gabon, Equatorial Guinea, Eritrea, South Sudan, Kenya, Uganda, Rwanda, Malawi, Zambia, Angola, Namibia, Botswana, South Africa, Eswatini.

Cameroon, Ethiopia, Lesotho, Sierra Leone, Tanzania, Republic of Congo have all formally banned crypto, with Liberia and Zimbabwe having introduced an implicit ban. The Bank of Central African States also introduced a ban on crypto for financial transactions in the Economic and Monetary Community of Central Africa, of which the Central Africa Republic (CAR) is a member. However, Bitcoin was decreed as the second official currency in CAR. Kenya, Nigeria, and South Africa have the highest number of crypto adopters.

Middle East

There appears to be a significant movement toward crypto regulation in the Middle East. This is the region with the fastest rate of crypto adoption, with the government looking to apply its underlying technologies to monitor financial activity and modernize markets. However, some analysts have argued that Bitcoin use by citizens is kept quiet "due to harsh government policies towards Bitcoiners."

Crypto payments are banned in Turkey, but it remains one of the biggest markets for crypto in the region. It is technically illegal to process crypto payments. However, Bitcoin and Tether are popular alternatives to the traditional financial system. Some Saudi Arabian women secretly use Bitcoin instead of traditional bank accounts, and Abu Dhabi, Dubai, and Bahrain are working to regulate crypto firms.

What does this mean for your firm?

Given the number of regulatory changes being introduced around the world, it is essential that firms build horizon-scanning activities into their day-to-day operations to pick up changes that are likely to impact their operations. As part of this process, firms will need to plan when they will need to update policies, processes, and systems. This will vary depending on the number of jurisdictions in which firms offer their services. Firms should also take into account the need to obtain additional resourcing as required to allow them to meet new obligations while ensuring that their systems and controls are relevant and remain fit for purpose. Firms should ensure that they have an open line of communication with their supervisor to understand when they will start assessing compliance with key changes and plan accordingly.

Firms operating in the crypto space will need to understand which countries are introducing provisions requiring them to be registered or licensed in jurisdictions where they offer services. Teams will need to ensure that they have the right documentation and that senior managers are "fit and proper" to run crypto firms and the AML/CFT department of crypto firms. Firms looking to get licensed - or who are recently licensed - will need to ensure that they have comprehensive AML/CFT programs, including enterprise-wide risk assessments, customer due diligence, sanctions screening, transaction monitoring, suspicious activity reporting, training, assurance testing, and record keeping.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

Regulatory themes

Filling crypto regulatory gaps

Firms operating in the crypto space have been calling on governments and regulators to clarify and "fill gaps" in regulation. Our survey shows firms operating or planning to operate in crypto globally have big plans.

When asked what crypto-based services they would offer in the future, 60 percent told us crypto as a payment method or rail, 55 percent a trading or exchange service, and 47 percent a custodian or wallet service. What's more, in almost all jurisdictions, firms plan to seek their own license rather than partner or integrate with a licensed firm.

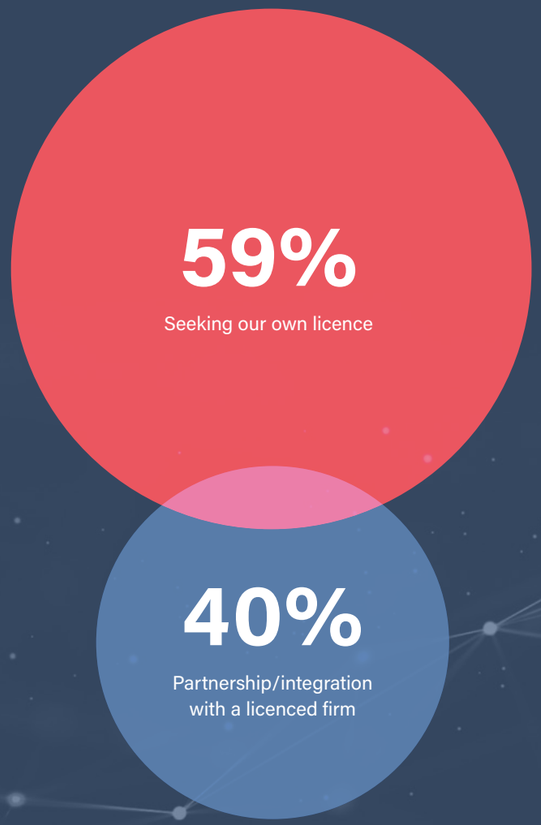
Globally, 59 percent of firms plan to seek their own crypto license. The only jurisdiction we surveyed where this didn't apply was Hong Kong, where just 36 percent plan to seek their own license, compared to 64 percent who plan to opt for a partnership or integration model.

In the UK, the crypto industry has been calling on Prime Minister Rishi Sunak to provide more clarity on crypto regulation, but also to accelerate licensing approvals. Sunak had previously indicated that he was "determined" for the UK to be "the jurisdiction of choice for crypto and blockchain technology." In Europe, firms are waiting for the Markets in Crypto Assets Regulation (MiCA) to pass.

This would not only provide clarity for firms on market entry requirements for crypto but would also introduce passporting provisions to allow for firms regulated in one jurisdiction to be passported to other EU member states. Globally, firms are seeking clarity to prevent regulatory arbitrage, and to address de-risking by banking institutions. Clearer standards and a more uniform approach to regulation could lower operating costs and generate trust in licensed, regulated crypto asset firms.

With respect to offering crypto asset services, what is your organization's licensing strategy?

Source: ComplyAdvantage, State of Financial Crime 2023



What crypto-based services is your organization planning to offer in the future?

Source: ComplyAdvantage, State of Financial Crime 2023

Growing regulatory focus on NFTs, stablecoins, and DeFi

The collapse of crypto firms, including Terra/Luna and FTX, has triggered an increased regulatory focus on NFTs, stablecoins, DeFi, and other unregulated virtual asset financial products. Countries, such as the US and Canada, are looking to introduce regulatory regimes for stablecoins. The Monetary Authority of Singapore also issued a Consultation Paper on Proposed Regulatory Approach for Stablecoin-Related Activities laying out its approach and requirements to be imposed for firms issuing and providing intermediation activities of stablecoins. South Korea appears to be leading the way and is anticipated to have a comprehensive crypto framework by 2024. The framework will include guidance on NFTs and ICOs and look to develop a CBDC. The country has also indicated that it will issue guidelines for security tokens. Also, in September 2022, South Korea proposed adopting the Metaverse Industry Promotion Act to support the metaverse development in South Korea, which is unique in the world. Following this announcement, the administration is set to issue the Digital Asset Basic Act (DABA).

Beneficial Ownership and Corporate Transparency

Countries around the world will continue to grapple with how to implement beneficial ownership transparency requirements. This includes deciding whether to create publicly available registries, determining who can access private registries and how to balance the competing needs for beneficial ownership information and data protection.

In December 2022, the US issued a Proposed Notice of Rulemaking defining the categories of persons who can have access to the federal register. The European Union's forthcoming AML reform package clarifies rules on beneficial ownership and how countries should detail who can access beneficial ownership registries.

A recent case in Luxembourg has created some challenges by ruling that access to beneficial ownership information by the public could be a data protection breach. Countries in Europe and around the world are assessing the impact of this legal finding and what this will mean for their beneficial ownership registries. In the UK, the Economic Crime and Corporate Transparency Bill will introduce provisions to address weaknesses identified in Companies House, including amendments to Limited Partnerships, clarity around who can register a company, and increased powers for the Registrar. Switzerland is also set to have a centralized beneficial owners registry by June 2023.

Corruption

Countries worldwide have been emphasizing anti-corruption initiatives, linking drivers of corruption to national security threats. The US is due to co-host the 2nd Summit for Democracy in March 2023 to promote democracy at home and abroad and to develop common approaches to tackling cross-border corruption. Work is ongoing to identify money laundering linked to corruption and to address challenges such as whistleblower protection. One focus is on the use of Strategic Lawsuits Against Public Participants (SLAPPs), a tool that oligarchs and criminals have increasingly used against investigative journalists.

Civil society figures are also raising awareness of poor enforcement of the OECD Anti-Bribery Convention, which has been in place for over 20 years. Transparency International launched a project to strengthen enforcement of the OECD anti-bribery convention, given the low enforcement rates of foreign bribery laws in OECD countries. In November, Glencore pleaded guilty to bribing officials to the tune of $29 million to gain preferential access to oil fields in Africa. UK authorities fined Glencore $280 million. NPOs have raised the need to go further and charge executives involved in bribery cases.

Tax Evasion and Transparency

There continues to be a push for more transparency in corporate tax arrangements. It is estimated that corporate tax abuse leads to losses of at least $483 billion annually. The G20 agreed to a minimum global tax of 15 percent for multinational corporations in 2021, and countries around the world continue to develop domestic frameworks to implement this.

At the United National General Assembly in November 2022, the Africa Group put forward a resolution calling for "inclusive and effective tax cooperation," laying the groundwork for members to develop a new UN convention on tax and giving the UN the mandate to "monitor, evaluate and determine global tax rules and support the establishment of a global tax body."

The European Council agreed on a directive to implement pillar two of the OECD's tax reforms, introducing a minimum global tax of 15 percent for companies with a combined turnover of EUR750. This will address base erosion and profit shifting and ensure that companies pay tax where it is earned. Individual countries are also looking at improving tax transparency. For example, Australia is looking at requiring more detailed reporting by corporates.

As part of its 2022/2023 budget, the government has introduced a multinational tax integrity package detailing anti-tax avoidance rules to minimize the risk that global entities with global revenue of at least AUS$1 billion claim tax deductions in no-or low-tax jurisdictions. Measures will be effective from July 1, 2023.

What does this mean for your firm?

"Firms must continue to ensure that they are aware of global regulatory themes and assess how looming changes and trends will likely affect them. This may include developing separate workstreams and projects to manage new changes. However, updates to existing policies and procedures may also be sufficient to enable the appropriate levels of due diligence and to identify suspicious behavior.

As regulations evolve, firms should carry out risk assessments as needed, adopting changes and monitoring regulatory news for further updates. Compliance teams should also identify jurisdictional touch-points, carry out gap assessments against coming changes and update policies, processes, and systems to address identified gaps."

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

← Previous section
Back to contents →

Industry Trends

From the rise of fintech and digital banking to the growing prevalence of cybercrime and fraud, the pressure on firms to be agile has never been higher. Our survey reflects this, showing that firms are increasingly aligning technological transformations with structural reforms within their organizations, focusing on legacy system updates and better cross-team collaboration.

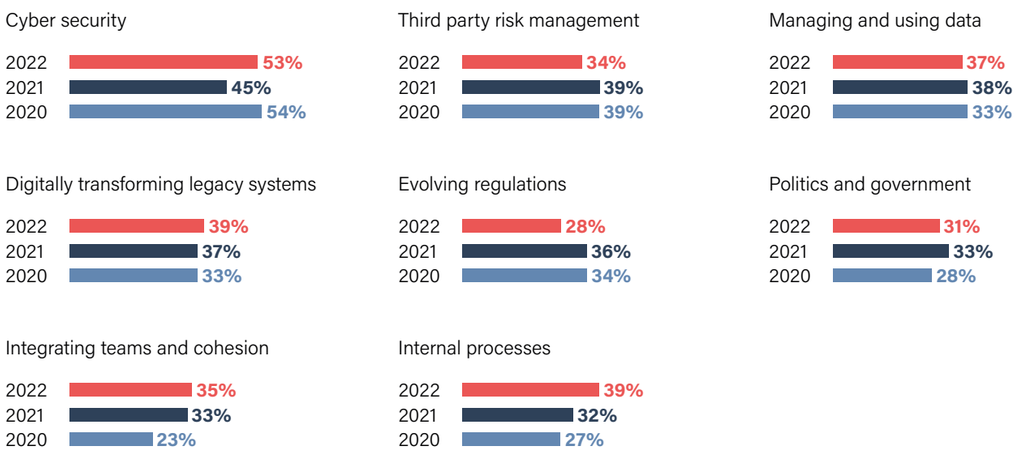
Technologies such as artificial intelligence (AI) are also becoming increasingly popular as more firms adopt an integrated mindset regarding fraud and anti-money laundering ('FRAML'). While compliance teams have been exploring the benefits of AI for some time, this year's data shows a clear shift towards assessing more specific use cases.

Firms focus on aligning technological and organizational transformation

Amidst challenges related to managing customer data, ever-increasing regulatory expectations, and competitive pressure, there has been a growing recognition among firms of the need to 'get the fundamentals right.' How? By ensuring they have a fit-for-purpose underlying framework to facilitate future success. For the compliance function, this means how their data and teams are structured.

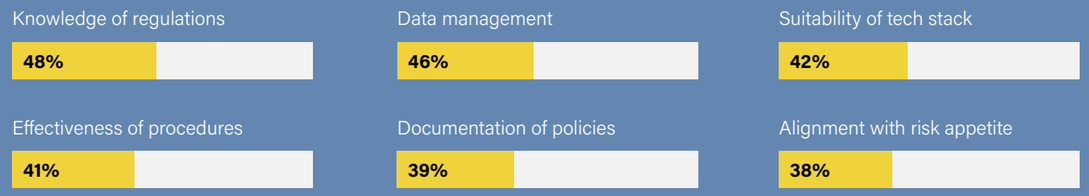
Firms increasingly recognize the imperative nature of these fundamentals as they learn dynamic, real-time systems, and experienced professionals cannot be layered on top of a substandard infrastructure. So, rather than relying on archaic, legacy systems often sustained by large teams and manual execution, many firms are shifting their focus to a more holistic view that aligns tech transformations with organizational changes.

In general, which of the below are your organization's biggest compliance-related pain points?



Source: ComplyAdvantage, State of Financial Crime 2023

If your organization was about to face a compliance audit, which areas of the compliance function would be 'at risk'?



Source: ComplyAdvantage, State of Financial Crime 2023

Our data corroborate this trend, with more firms than ever telling us that digitally transforming legacy systems - alongside integrating teams and cohesion - are pain points.

39 percent of firms said digitally transforming legacy systems was their most significant compliance-related pain point, a two percentage point increase on 2021 and 6 percentage points higher than in 2020. This trend is likely self-reinforcing, with compliance officers moving between different financial institutions able to compare newer, more sophisticated tech stacks with older ones. As a result, they become more aware of legacy technologies' limitations and more determined to implement modernization initiatives where they are needed. Indeed, when asked which area of the compliance function would be 'at risk' in an audit, 46 percent cited 'data management,' with 42 percent saying the suitability of the tech stack and 41 percent the effectiveness of procedures.

Furthermore, firms also cited 'relevancy' as a critical challenge with respect to data. Specifically referring to data being stored in the correct categories, 38 percent of firms said this was their organization's most significant pain point alongside compiling global data. Not only does this represent a seven percentage point increase from 2020, but it also correlates with the growing concerns about legacy systems - as good data hygiene is only feasible when systems are able to support it.

While technology is a powerful tool that can streamline operations, reduce costs, and increase customer satisfaction, more firms recognize it can lead to inefficiencies and extra costs if it is not adequately integrated into the organizational structure. By collaborating and leveraging the team's collective knowledge, organizations can make the most of their data and make the best decisions for their business.

When asked how they planned to respond to the uncertain global economic environment, almost 60 percent of firms said they were preparing for a general rise in financial crime and intended to increase the number of staff within their compliance teams.

When asked how they planned to respond to the uncertain global economic environment, almost 60 percent of firms said they were preparing for a rise in financial crime and intended to increase the number of staff within their compliance teams.

As financial crime techniques and technologies become more sophisticated, compliance teams may require a more dynamic range of skills to ensure their controls remain appropriate and relevant, including data science and digital forensics. As discussed in the 'Spotlight on Financial Crime' section of the report, the rise of super apps will also heighten the demand for skilled compliance staff, making a hot hiring market even more sizzling.

To combat this, firms should assess where skilled time is spent within their compliance departments and consider the potential of automated AI to free-up time and reduce the pressure to hire new people as firms scale.

What does this mean for your firm?

Many firms have long known that their existing technology stacks - either due to immaturity or a reliance on legacy platforms - cannot help them to scale while meeting customer and regulator expectations. Our survey data suggests 2023 is the year firms decide to do something about this long-standing problem. But with so much focus on the bottom line in the year ahead, compliance teams need to be disciplined in their approach to upgrading systems and reorganizing teams. Set clear goals and expectations, aligned to wider business objectives, and be realistic about how quickly change can happen. Equally, firms shouldn't be afraid to explore new vendors and conduct an extensive RFP process if their existing suppliers won't deliver.

Alia Mahmud
Regulatory Affairs Practice Lead, ComplyAdvantage

Are firms becoming desensitized to the threat of fines?

For the third consecutive year, there was a notable percentage point rise in the number of firms telling us they choose to incur AML fines and make violations "all the time." This number, 61 percent in 2020, had risen to 79 percent by 2022. While overall regulatory enforcement action remained the event most likely to drive change in organizations, the percentage saying so fell by one point to 38 percent.

This could be driven by the small fines relative to firms' turnover and the lack of criminal enforcement actions against individuals in senior management roles. However, the former CEO of Swedbank has begun a criminal fraud and market manipulation trial in 2022. There is some evidence that firms believe greater accountability is essential, with 38 percent of respondents saying "personal liability for the C-Suite" is an area of AML regulation that needs to be strengthened. Similarly, "larger fines for AML violations" was chosen by 40 percent of respondents. While this represents a drop compared to 2021, it remained one of the top three answers, indicating accountability, and the reputational damage hefty fines and executive prosecutions bring with them could be an area firms would like to see progress on.

There is some evidence that firms believe greater accountability is essential, with 38 percent of respondents saying "personal liability for the C-Suite" is an area of AML regulation that needs to be strengthened.

What does this mean for your firm?

There are clear indications of 'enforcement fatigue' in this year's survey. More than ever, compliance officers will need to keep their businesses focused on good outcomes by emphasizing the human, as opposed to financial, cost of financial crime. Indeed, firms should not be complacent about the longer-term reputational effects of widely-publicized fines and enforcement actions, particularly with the oldest of the millennial generation starting to enter middle-age.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

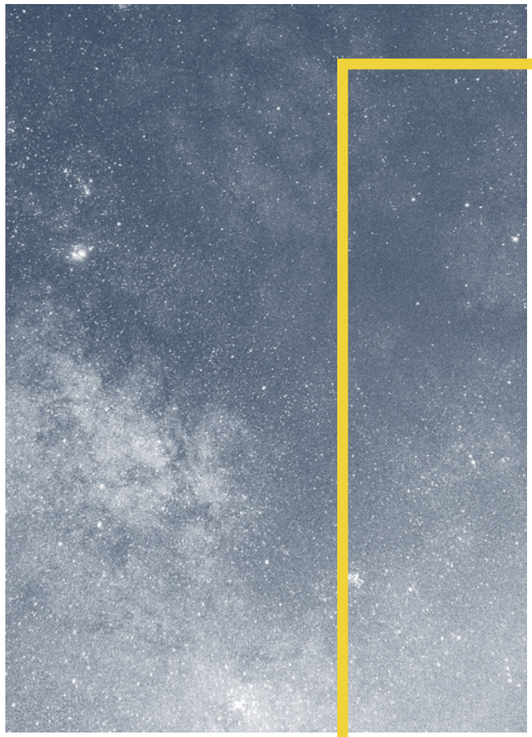
AI for financial crime risk detection: From exploration to implementation

AI is fast becoming a core feature in cutting-edge regulatory technology. Competitive firms have spotlighted their reliance on artificial intelligence and machine learning (ML) as key to their success. A 2022 report by Allied Market Research predicted that the market for fintech AI would reach over $61 billion by 2030. The piece discussed top global firms' use of AI for fraud prevention, biometrics, process automation, and agile data analysis. Once relegated to speculation, AI and ML are increasingly practical realities – judging by worldwide regulatory responses, their use is becoming ubiquitous. Key examples include:

- The European Union's proposed Artificial Intelligence Act
- US House Committee on Financial Services' Task Force on Artificial Intelligence
- The United Kingdom Financial Conduct Authority's AI Public-Private Forum and Artificial Intelligence Discussion Paper
- The Monetary Authority of Singapore's Project Veritas

Efficient and accurate data analysis is vital for effective AML/CFT programs. As global financial crime trends continue to rise, compliance teams face growing datasets that outpace traditional tools even while budgetary and staffing pressures increase.

But with artificial intelligence, vendors have begun to offer solutions with far superior capabilities that seamlessly address this dilemma. In a recent interview, PwC Luxembourg's Andreas Braun highlighted how fintech companies now leverage artificial intelligence in AML and know-your-customer (KYC) processes. In particular, he emphasized the tremendous data processing and analysis possible through AI, which helps solve traditional risk management efficiency and cost dilemmas. Artificial intelligence is quickly becoming a staple in the financial compliance sector thanks to its power and elegance.

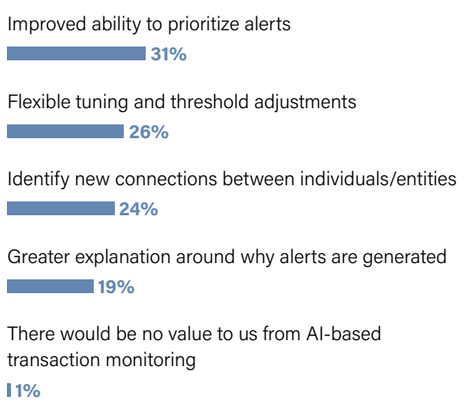


What does this mean for your firm?

"At ComplyAdvantage, our conversations with prospects and customers around AI have certainly reflected the trends identified in our industry survey. Compliance officers understand the potential of AI, and come to us with specific use cases they would like to address. Once a use case has been identified, an important starting point is always a proof of concept. This will help project leads to focus minds and secure buy-in from key stakeholders. Equally, many firms are already seeing success with AI, so it's important to be agile, and avoid falling behind competitors who may soon be able to work in a much more sophisticated way without comparable increases in costs."

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

Which of the following benefits of artificial intelligence (AI)-based transaction monitoring would add the most value for your organization?



Source: ComplyAdvantage, State of Financial Crime 2023

The survey data bears this out. 99 percent of surveyed firms expect AI to impact financial crime risk detection positively. They anticipate specific gains in transaction monitoring. When asked which transaction monitoring use case AI could best help them with, firms overwhelmingly identified three:

- **Alert Prioritization** – 31 percent of respondents expected AI to help rank transaction alerts by risk. This enables transaction monitoring teams to catch more risky activity and do it faster.
- **Flexible Tuning** – 26 percent thought they'd use AI to improve their alert system – helping to adjust thresholds and fine-tune alerts responsively.
- **Relationship Identification** – 24 percent anticipated artificial intelligence would uncover new relationships between monitored entities and individuals.

Only one percent of the respondents didn't expect AI to benefit their transaction monitoring.

Firms wishing to adopt artificial intelligence to enhance their existing processes could start with a gap analysis. What areas are struggling most to meet robust AML/CFT standards?

Many firms' hard-coded rules are inefficient – overloading analysts with false positives while failing to identify dynamic risks. Once the most pressing inefficiencies are identified, companies can consider how best to address them with machine learning or artificial intelligence. For example, Deloitte has noted that some firms use intelligent alert prioritization to increase their hard-coded rules' efficiency to address false positives. In one use case, prioritization reduced false positives by a third (33 percent). If a firm's gap analysis reveals detection failures, it can use AI to uncover hidden risks by seamlessly layering advanced techniques like behavioral analysis and anomaly detection.

However it is done, the implementation of AI requires sensitivity, reflecting wider issues around data quality and organizational change flagged in this report. Any large scale deployment of AI in transaction monitoring - or across an AML/CFT program more widely - needs to be properly integrated with existing teams, processes, data and platforms to ensure firms get the best outcomes.

PEP screening sophistication increases

With politically exposed person (PEP) regulations varying globally, discerning global trends in how compliance teams approach PEP screening can be complex. This year's survey, however, showed a clear shift toward a greater focus on mid-level government officials. When asked which area their firm most valued in a PEP screening solution, 39 percent said mid-level government officials, a ten percentage point increase on 2021 that made it the highest ranking factor.

When assessing PEP (Politically Exposed Person) screening solutions, what area does your organization most value?

Global coverage

2022 38%
2021 39%

RCAs (Relatives and Close Associates)

2022 34%
2021 31%

Mid-level government officials

2022 39%
2021 29%

Source: ComplyAdvantage, State of Financial Crime 2023

The data shows that firms increasingly recognize that there is no "one size fits all" classification when it comes to PEPs. In particular, there is a recognition that middle-ranking and even more junior officials could act on behalf of a PEP, circumventing AML/CFT controls. As a result, it's entirely appropriate for firms to cover these less prominent public functions as customer risk factors as part of their enterprise-wide risk assessments, especially when they have exposure to high-risk jurisdictions.

Enforcement of the US Office of Foreign Assets Control (OFAC) 's so-called '50 percent rule' could also be driving this shift. A growing focus on ultimate beneficial owners (UBOs) means firms widen their nets as they try to capture PEP risk in their UBO populations.

More widely, growing political instability - and the impact this has on firms' risk appetites, as we explored in the 'Spotlight on Financial Crime' and 'Geopolitics and Sanctions' sections of this report - could also be driving greater PEP caution. This trend will continue in 2023. For example, lower-level PEPs who may be removed from consideration in politically stable countries could now be increasingly included in firms' ongoing monitoring processes.

What does this mean for your firm?

"Every compliance officer knows the importance of embedding a risk-based approach. Understanding the different risk factors of PEPs and assessing them independently is an important part of a truly risk-based AML program. As many firms become more risk averse, however, they will also need to assess other risk control factors: How fuzzy should our search settings be? Should PEP screening occur weekly instead of monthly to account for political volatility? Is it necessary to recalibrate the way domestic vs foreign PEPs are managed?

A deeper understanding of the political environment and the vulnerability of the PEP's country of political exposure to corruption will unearth these questions. Compliance teams should consult guidance from their local regulators, discuss their approach internally, and with experts at any vendors and partners they work with to benchmark how other similar firms are approaching these issues."

Alia Mahmud
Regulatory Affairs Practice Lead, ComplyAdvantage

KYB solutions evolve to meet market expectations

As AML regulations expand and business relationships grow more complex, firms are seeking to bolster an essential aspect of customer due diligence: know your business or KYB. KYC has often been the natural primary focus when considering global CDD requirements. But equally important are business-to-business relationships, which also fall under the CDD legislative scope. The UK's Financial Conduct Authority (FCA) and the European Banking Authority (EBA), for example, leave their definitions broad, calling for due diligence on "business relationships."

The Wolfsberg Group's 2022 Financial Crime Principles for Correspondent Banking further illustrate KYB's importance among CDD practices. The inherent liability involved in a correspondent relationship requires firms to verify the prospective business, its processes, and its regulatory accountability with enhanced due diligence.

In this year's survey, more than a third of respondents – 34 percent – said they planned to replace or upgrade their KYB solutions. In 2021, Fatpos Global projected a market increase in electronic KYB from around $150 million in 2020 to over $533 million by 2030. Alongside global regulatory trends, this interest is partly thanks to a rise in tailored vendor offerings powered by next-generation tech.

KYB solutions solve pressing industry problems. A 2022 PYMNTS study tied inadequate KYB to substantial fraud-related losses – including resources wasted on false positives. In contrast, firms using "proactive and automated solutions" experienced losses lower by roughly 34 percent. Nearly half of the surveyed organizations struggled significantly with digital business identity verification. The study identified an over-dependence on legacy solutions and limited resources among key factors holding firms back.

The report recommended, among other things, streamlined onboarding technology that could balance efficient ID verification with risk considerations. Technologies such as artificial intelligence, biometrics, and REST APIs allow businesses to streamline and integrate KYB with broader risk management services. APIs, in particular, enable firms to layer approaches like ID verification, digital forensics, behavioral analytics, and identity clustering to ensure powerful, specific risk management. Known as orchestration, this multifaceted approach allows firms to target bad actors more effectively while making processes smoother for legitimate customers. It also allows firms to merge traditionally compartmentalized processes, such as KYB onboarding and FRAML monitoring, into a more cohesive and risk-responsive package.

What does this mean for your firm?

KYB has for too long been the white whale of financial compliance - everyone understands why it's important, but the technology available has often fallen short of what is required. Advances in the solutions offered by vendors mean this is no longer the case. But it's important to see KYB as part of a wider shift away from siloed compliance processes. Firms should look for solutions that combine corporate and risk screening, and provide a holistic picture of the challenges they face. As our survey data has shown, adding another siloed solution to the compliance tech stack is the last thing teams need or want.

The European Court of Justice's November 2022 challenge to the requirements in the 5th Anti-Money Laundering Directive (AMLD) around the creation of national beneficial ownership registers was seen as a blow by many with a vested interest in improving the KYB landscape. However, the long-term effect of this challenge likely be to tighten the access rights to registers to those with a demonstrable interest in the prevention and detection of crime, including those involved in the collection of customer due diligence.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

ESG and corporate credibility take center stage

Due to the growing importance of sustainability in the global economy, more firms are prioritizing an Environmental, Social, and Governance (ESG) program and building corporate credibility among regulators, customers, and the public at large. The factors fuelling this shift are undermined by a growing awareness of environmental crime risk, emerging legislation, and becoming increasingly aware that firms' reputations need to be proactively protected.

As discussed in the 'Spotlight on Financial Crime' section of the report, environmental crime has become one of the most profitable and fastest growing areas of international criminal activity, with one in four firms selecting it as a critical predicate offense to screen against. However, the impacts of environmental crime go far beyond economic costs. In addition to adversely affecting life support systems and threatening biodiversity, firms are increasingly subject to reputational damage if they lack awareness or understanding of the importance of ESG criteria and their role in mitigating financial crimes.

Since AML failings can cause firms to suffer an average 21 percent slump in their share price, it is unsurprising that 34 percent of firms cited 'reputational damage' as the event most likely to drive change within their organization. This represents a six percentage point increase from 2021, overtaking 'competitor threats' as a top concern. These results reflect a change in the economic landscape, which has become increasingly punctuated by scrutiny from the media and regulators regarding corporate conduct and culture.

of millennials (those born between 1981 and 1996) are "eco-conscious to the point of changing their buying habits to favor environmentally friendly products."

Source: Nielsen

These results also point to the importance of garnering consumer trust in a volatile market. According to Nielsen, 75 percent of millennials (those born between 1981 a nd 1996) are "eco-conscious to the point of changing their buying habits to favor environmentally friendly products." Therefore, firms implementing ESG programs with transparency and integrity will likely attract the business of the largest group of consumers currently in the market, as well as top talent seeking to work for organizations that prioritize sustainability.

While understanding and managing an organization's exposure to environmental crime is a critical pillar of an ESG program, regulators are also intensifying their focus on ESG criteria. Examples include:

- The US Securities and Exchange Commission (SEC) is proposing amendments to rules to regulate ESG disclosures for investment advisers and investment companies
- The Financial Conduct Authority (FCA) is proposing new measures to clamp down on 'greenwashing,' including restrictions on how terms like 'ESG,' 'green,' or 'sustainable' can be used
- The Monetary Authority of Singapore (MAS) and Singapore Exchange (SGX Group) are launching a digital disclosure portal for companies to report ESG data
- The European Banking Authority published its Roadmap to Sustainable Finance, explaining how it plans to approach the integration of ESG risk considerations into the banking framework over the next three years.

What does this mean for your firm?

"Right now ESG is something of a wild west - everyone is trying to show they're doing it, but without the guardrails regulations provide, inevitably some providers are doing better than others. As a result, firms should expect more regulation around ESG in the year ahead, and should keep abreast of the latest announcements in their jurisdictions in case additional due diligence on their customers is required."

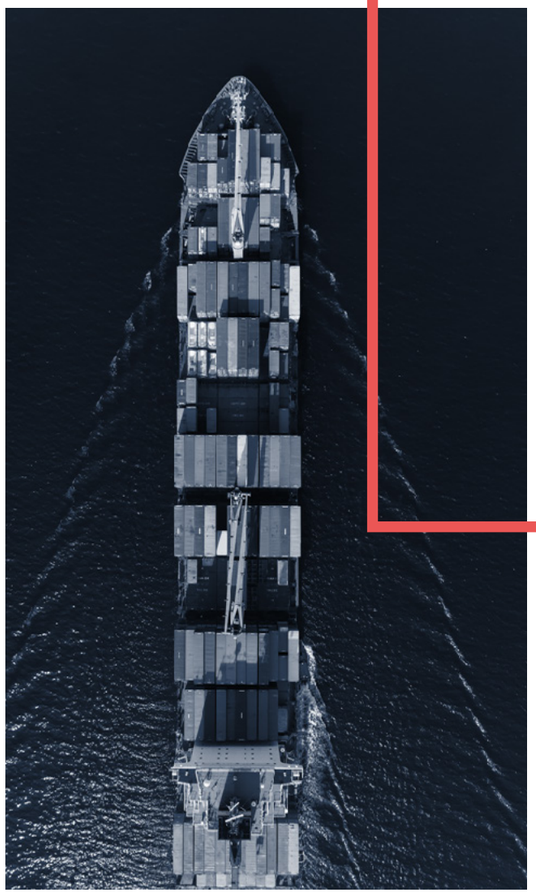
Alia Mahmud
Regulatory Affairs Practice Lead, ComplyAdvantage

Supply chain risk becomes an integrated part of AML compliance programs

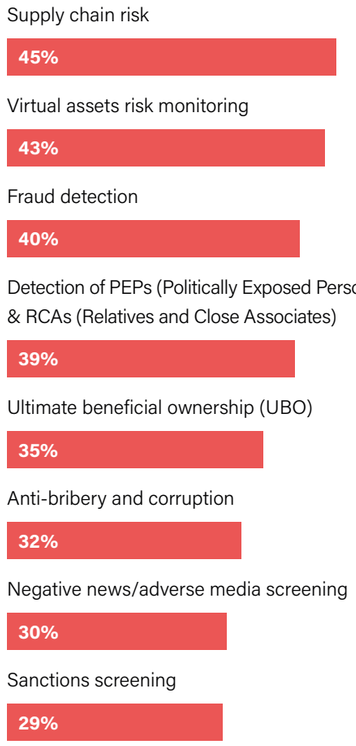
Having experienced sustained disruption through the pandemic, firms are now looking to build their long-term resilience to supply chain disruption. While immediate post-pandemic supply issues have eased through 2022, it's clear firms are taking no chances. The ongoing war in Ukraine, high tensions with China, and new additions to the FATF blacklist, including Myanmar, all contributed.

Nearly half of financial institutions - 45 percent - recognized the need to integrate supply chain risk management into their AML programs. Among all categories of improvement surveyed, this new category was the highest of concern this year. It's also unsurprising, given how supply chains have become increasingly entangled in the intense geopolitical polarization between the US and China – leaving them vulnerable to sudden disruption.

As the complexity and importance of supply chains have increased, so too has regulators' focus on operational resilience. Multifaceted by nature, operational resilience is sometimes combined with other regulatory concerns, such as financial crime risk management. Firms are seeking to keep up as regulators worldwide continuously adapt their requirements to the changing global ecosystem.



Specifically thinking about AML compliance, which area is your organization most focused on improving?



Source: ComplyAdvantage, State of Financial Crime 2023

In sectors where the supply chain is complex, disruptions can have a ripple effect on multiple industries. In December 2022, for example, the Biden administration announced plans to blacklist Yangtze Memory Technologies (YMTC), along with 30 other Chinese technology companies, after months of pressure from lawmakers to place the chipmaker on the entity list. Companies based in the US will only be permitted to supply the chipmaker if they obtain an export license. This follows an ongoing struggle between the US and China, in which the United States seeks to limit China's development of technology with military potential. The US also seeks to enter a similar accord with the Netherlands and Japan. The agreement would prevent companies under all three jurisdictions from exporting chipmaking supplies to China.

As international sanctions continue to develop, the risk of sanctions violations is exceptionally high. Even early on, Russian sanctions hit the global supply chain hard, and the program's global effects will continue as regulations become more stringent. Within ten days in December 2022, Canada, the United States, the United Nations, and the United Kingdom all applied new sanctions against Russia and Russian entities. For example, the UK prohibited broad-ranging services to "a person connected with Russia" that included advertising, engineering, architecture, and information technology, as well as restrictions broadly impacting the financial services sector. The United States' updated SDN list means "non-US persons" can face secondary sanctions risks if they are found to have provided SDNs with "material support." And there is no sign these rapid changes will slow any time soon.

Far-reaching sanctions always lead to the risk of evasion attempts. Yet the current ecosystem is one in which regulators and perpetrators compete to stay ahead of one another, creating a landscape that evolves at a staggering pace. Companies reviewing their approach to supply chain risk management must ensure it is holistic and continually updated. This means, of course, constantly aligning with new sanctions to prevent non-compliance. But it also means firms should take a structured and comprehensive view of their supply chains and everything connected to them. This includes considering methods used to fly under the radar of sanctions, such as blockchain-based currencies.

Such a holistic approach requires robust, regularly updated risk assessments, ensuring efforts are focused in the most effective areas and do not become outdated. These risk assessments should take compliance vendors into account, too. As with any other business partner, they should also be subject to continuous due diligence.

The support of proper technology is increasingly vital to reliable risk management. Firms should audit their existing tools to ensure they support a risk-based approach. Emerging layered technologies are more reliable than depending on one or two methods for screening and monitoring. These orchestrated approaches use machine learning and APIs, combining multifaceted techniques into one powerful yet streamlined process.

What does this mean for your firm?

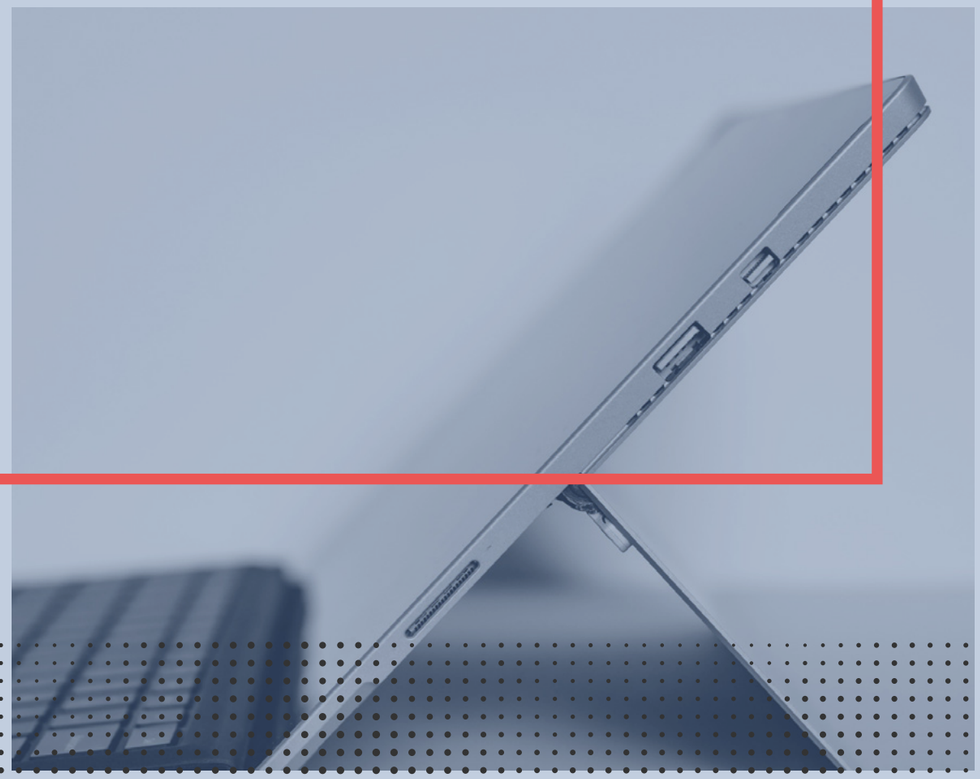
Supply chain due diligence was a hot topic in last year's report, for 2023 it's clearly an established trend, and an essential part of business operations. With tensions still high with China - a much bigger part of global supply chains than Russia - firms will need to consider a blanket approach to enhanced due diligence for relationships with even a tangential nexus to those jurisdictions. To refer again to the significance of KYB, firms with corporate customers will need to pay attention to any potential ties those customers may have to supply chains involving the fabrication of semiconductors, silicon wafers, and related technologies.

In addition to understanding the current nature of supply chains, firms also need to assess the potential impact of sudden changes, and ensure they have as much resilience built into their processes as possible. At minimum, if disruption is inevitable, wherever possible, it should be expected.

Iain Armstrong
Regulatory Affairs Practice Lead, ComplyAdvantage

Explore more of our content at complyadvantage.com/insights

and subscribe to our weekly AML newsletter
complyadvantage.com/newsletter-signup



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

Santander · GEMINI · OakNorth Bank · CURVE · raisin. · Munich RE · Lydia · OANDA

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