The State of
Financial Crime 2022

COMPLY ADVANTAGE®

Contents

Executive Summary

Financial Crime Threat Landscape

Criminals will continue to adapt and exploit opportunities to grow and evolve as the world continues to contend with COVID-19 and emerging variants. Dominant themes of the "new reality" this year will include disrupted supply chains, the implosion of fraud, widespread ransomware attacks and a digital payments ecosystem under continual attack by criminals.

Takeaway

Firms should review their business risk assessments to identify emerging threats. They should also update policies and processes to help prevent and detect financial crime in their organizations.

Geopolitics and Sanctions

The tense, rapidly changing geopolitical landscape will see the release and removal of sanctions as Western powers face off against China and Russia, coups take hold of fragile states and new sanctions measures introduced to tackle the misuse of technology by nefarious actors.

Takeaway

Firms should ensure that they have robust adverse media, sanctions screening and payment filtering systems in place in order to identify any changes made to sanctions lists as political events impact the addition or removal of economic, trade and financial sanctions.

Regulatory Trends and Enforcement

In 2022, the massive overhaul of regulatory frameworks will continue as Europe, the US and others work to bring greater legal definition to crypto firms. Measures will also be designed to prepare for upcoming FATF evaluations and/or address deficiencies that have already been identified to avoid being added to the gray list. Regulators will continue to step up fines to deal with firms that have deficient AML/CFT programs.

Takeaway

Firms should ensure that they keep an eye on the extensive regulatory changes taking place. They should also make sure they can update their AML/CFT systems and controls to remain up to date.

Industry Trends

With regulatory action and competitive threats driving change across the compliance industry, firms will continue to invest in new RegTech solutions in 2022. Alongside rising levels of automation, hiring the right staff remains critical, with banking the most sought-after industry background for firms that are recruiting.

Takeaway

Firms should continue to review their compliance tech stack, exploring how new technologies can deliver against their objectives, reduce data silos and help them to fully realize a risk-based approach. They should also assess the skills and experience of their in-house team to explore if/where new perspectives could add value.

Introduction

Welcome to ComplyAdvantage's outlook for 2022. From supply chains in crisis to high-wire geopolitical standoffs and the implementation of massive new regulatory frameworks, it's going to be a landmark year for compliance professionals.

In the final months of 2021, ComplyAdvantage interviewed 800 C-suite and senior compliance decision-makers across North America, Europe and Asia-Pacific. The respondents represented enterprise banking, investments, crypto, insurance organizations and fintechs. Their answers provide critical insights into the trends that will shape the year ahead. By looking back to the 2020 survey, for which we interviewed 600 people, it's also possible to explore challenges, problems and priorities that have risen and fallen over the last 12 months.

With much of the global agenda dominated again by the pandemic, it could easily be assumed that the compliance challenges identified this year will be similar to those featured in the 2021 report. However, whereas 2021 saw a focus on adaptation through a global pivot to remote working and major stimulus programs, 2022 will be the year of adjustment. One example of this in the survey relates to predicate offenses. When asked for the top predicate offenses firms are screening against in 2020, 61% cited fraud amid widespread reporting about fraudulent activity related to COVID-19 relief funds. By 2021, the percentage of respondents citing fraud had dropped dramatically to 37%. Instead, cybercrime was listed as the most important predicate offense firms are screening against, followed by tax crime.

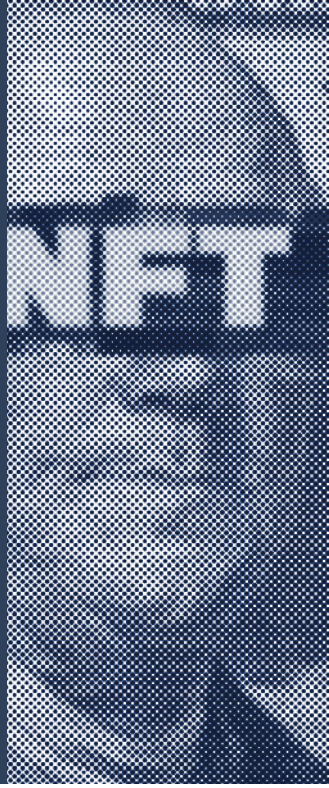
As these figures suggest, challenges outside of the pandemic are emerging. Following key sessions at COP26, as well as the G7 and G20 summits, it's likely environmental crime will be a major theme this year. Relations between the major Western powers, China and Russia will continue to be strained.

The regulation of crypto firms and virtual asset service providers (VASPs) will remain high on the agenda for 2022. This has been a core priority of the Financial Action Task Force's (FATF) German Presidency. With 98% of firms saying they're either crypto-native, accept/work with crypto or plan to offer crypto-based services in the future, how these are regulated — and the risk of arbitrage — is set to be a closely watched theme this year.

Another key focus has been the exploration and implementation of new technologies, which our survey indicates is also a top priority for firms globally. Organizations continue to look to upgrade legacy systems, manage their data more effectively and access AML risk data in real time. The number of firms saying real-time AML risk data would "significantly" improve their compliance operations increased by 15 percentage points in 2021.

Overall, in a year set to be defined by uncertainty and volatility, firms will need both a comprehensive risk-based approach and a willingness to reevaluate services, markets and customers at short notice.

Spotlight on Financial Crime



This section will explore how the financial crime and regulatory landscape will continue to be shaped by global trends and events in 2022, including the COVID-19 pandemic, supply chain issues, fraud and cybercrime, the world of cryptocurrencies, NFTs, and DeFi, and the evolving threat of both organized and decentralized terrorism.

The continued volatility of the financial crime landscape, alongside the rapid rise in new technologies and payment methods, was reflected in the 2021 survey (Figure 1). 80% of firms said they filed more suspicious activity reports (SARs) in 2021, compared to 70% who said the same in 2020. Almost a third of respondents (31%) said they filed 10–20% more SARs in 2021 compared to 2020.

Has the number of SARs that your organization filed changed in 2021 compared to 2020?

'ComplyAdvantage: The State of Financial Crime 2022'

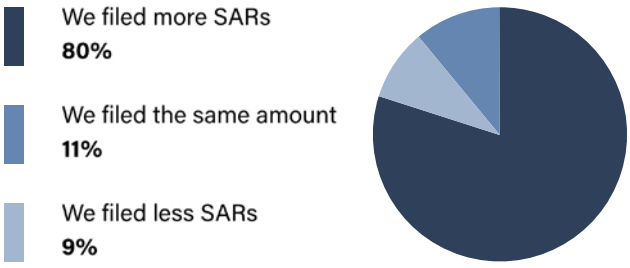


Figure 1

COVID-19 and the Nature of Work

The response to COVID-19 and its variants will continue to impact all facets of life, including society's relationship with the traditional workplace. Throughout 2020 and 2021, lockdowns, hiring freezes and remote working arrangements prompted many to reevaluate their priorities and what they want from their chosen job.

As a result, employees are leaving their jobs in record numbers. In the US, for example, a high of 4.4 million Americans quit their jobs in September 2021 — up from the high set the previous month of 4.3 million. In the UK, the number of estimated job openings climbed to over 1 million for the first time in July 2021. Further, a study conducted by Microsoft, published in March 2021, indicated the trend has gone global: around 41% of workers worldwide are thinking about leaving their current employer. Those in cybersecurity and compliance functions are not immune to this trend or its effects.

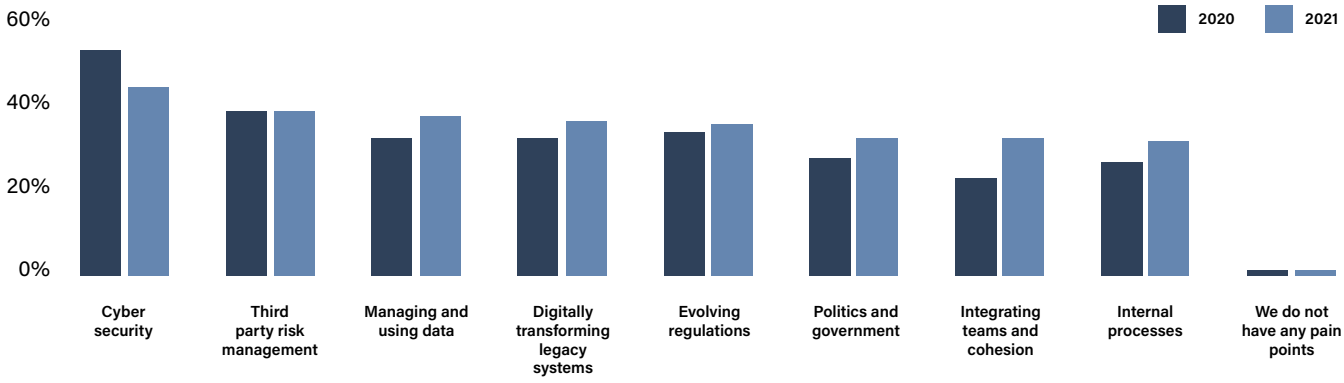
As the world continues to emerge from the pandemic, this trend, termed the "Great Resignation," will continue. High turnover rates leave businesses in a precarious position: failure to implement or follow proper onboarding and offboarding processes increases the risk of exposure to criminality, cyberattacks, data loss and theft, among others.

The proliferation of remote and hybrid working models is another trend to consider when assessing risk. Recent findings from KuppingerCole and HP Inc. confirm that the number of global cyberattacks increased 238% during the pandemic — and that remote workers are a prime target for hackers. Given that over 70% of employees are accessing more customer, operational, financial and HR data from home now than before the pandemic, and more are using their work devices for personal activities, it's easy to see why.

The 2021 survey data reflects these challenges. Cybersecurity remained the biggest compliance-related pain point (45%) for firms in 2021 (Figure 2). There was also a five percentage point increase in the number of respondents citing "managing and using data" as a concern compared to the 2020 survey. "Integrating teams and cohesion" saw the biggest percentage point change from last year, with a nine percentage point increase to 33%.

In general, which of the below are your organization's biggest compliance-related pain points? *Figure 2*

'ComplyAdvantage: The State of Financial Crime 2022'



Therefore, businesses don't just need to worry about vetting potential employees or securely offboarding former employees. Data breaches, insecure remote networks, risky employee behavior and human error must be controlled for and addressed as companies move to incorporate remote working into their long-term staffing and operational plans.

AML/CFT regulators are taking note, with "remote KYC" a key area of focus. The Monetary Authority of Singapore (MAS) and The Association of Banks in Singapore (ABS) issued a report in March 2021 exploring the AML/CFT risks created by increased levels of remote working. MAS noted, for example, that remote KYC creates a higher risk of fraudulent activity such as identity theft, and the forging of documents.

The MAS report builds on earlier guidance from Australia's regulator, AUSTRAC, on how to comply with KYC regulations during the pandemic. AUSTRAC includes recommendations on using alternative proof of identity processes and disclosure certificates for corporate customers. The documentation also addresses dealing with customers in isolation, customers with no access to technology, and situations in which front line staff are unable to verify documents as they would in person.

In November 2021, the UK's Financial Conduct Authority (FCA) released guidance on remote working for firms under its purview, highlighting the need to ensure that remote working doesn't "damage the integrity of the market" or "increase the risk of financial crime." The FCA also made clear that firms that do not implement and document the existence of sufficient safeguards in response to remote working will not be shown leniency if compliance gaps are detected. Other regulators will likely follow suit in 2022.

Finally, firms will need to address security challenges related to digital transformation and the adoption of disruptive technologies. Estimates place global digital transformation spending at $2.8 trillion by 2025 (up from an estimated $1.5 trillion in 2021), with companies increasingly incorporating artificial intelligence, blockchain technology, autonomous systems, automation and decentralized ledgers into their business models and processes. The opportunities for positive changes within the financial system are significant. But so are the vulnerabilities criminals can exploit. Safeguarding businesses and the global financial system will require proper risk management and employee upskilling.

What does this mean for my business?

Firms need to invest in their employees and take steps to provide and maintain a high level of job satisfaction. Regular training in information security threats is critical, as is ensuring that employees understand new technologies and can appropriately manage risks and opportunities. Firms must also manage risks around onboarding and offboarding employees — including having adequate vetting procedures in place and processes for swiftly locking IT access to former employees.

Supply Chain Shocks

COVID-19 has had a massive impact on global supply chains, with many areas vulnerable to criminals looking to exploit the disruption for their personal gain. Pandemic-induced quarantines in Chinese ports and deteriorating trade relations between China and Australia have been key drivers of supply chain delays. These issues were exacerbated by natural disasters, such as Hurricane Ida in the US and Typhoon Chanthu in China, alongside continuing shortages in key product areas, such as semiconductors.

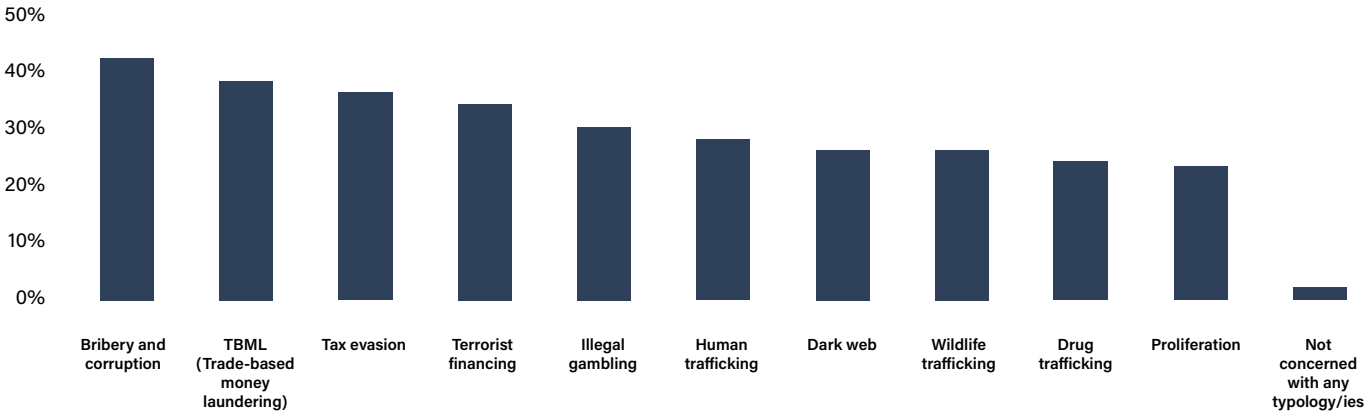
In China, cities and ports have found themselves in quarantine for up to seven weeks, with further controls likely in the first half of 2022. The "COVID-Zero" strategy also applies in Hong Kong, leading freight delivery firm FedEx to announce in November 2021 it would be shutting down its base in the region, and relocating personnel to California. Another area of pressure relates to feeder operators, who are responsible for transporting containers between small ports and major terminals. Operators announced an extension to the suspension of service operations lasting at least six weeks over the Lunar New Year holiday period.

The trade dispute between China and Australia has also escalated, with both countries filing complaints with the World Trade Organization over tariffs, and China looking to new markets to source embargoed goods. Australia, meanwhile, is continuing to search for new markets to counter the reduced trade with China. Such shifts could be exploited by criminal gangs, as customers scramble to source goods from new, potentially unknown suppliers.

One of the biggest impacts of supply chain shocks has been on the cost of shipping goods, which has soared in recent months. In Canada, for instance, the Burnaby Board of Trade reported that businesses experienced a jump in shipping costs of more than 400% from January to August 2021. Such massive increases in costs provide criminals with more opportunities to enter the shipping market and operate a number of trade-based money laundering schemes, including the over- or undervaluation of goods, the over- or undershipment of goods and false reporting on invoices, among others. When asked about the typologies they're most concerned with (Figure 3), 38% cited trade-based money laundering, making it the second most common answer. Only bribery and corruption generated a higher response rate.

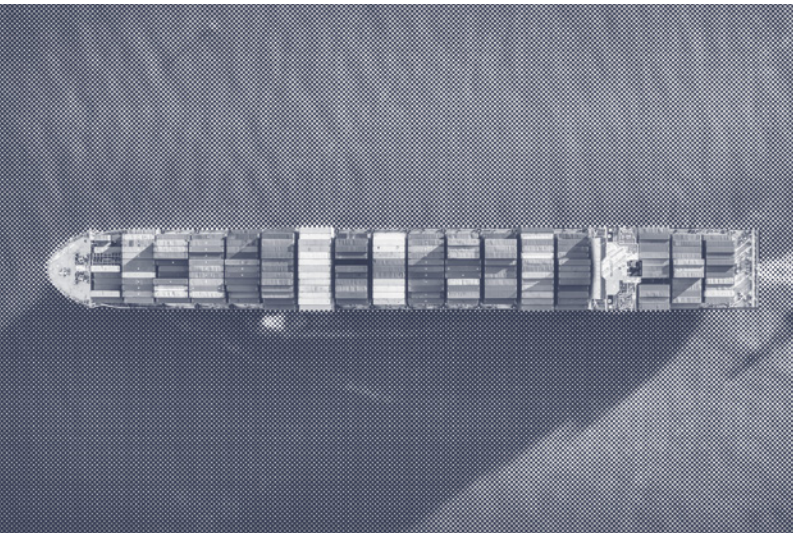
When submitting suspicious activity reports, what typology/ies is your organization most concerned with? *Figure 3*

'ComplyAdvantage: The State of Financial Crime 2022'



Indeed, the British Standards Institution (BSI), a leading supply chain intelligence firm, confirmed that crime syndicates created front companies in warehousing, transportation and distribution in 2021 and found that there has been an increase in fake carriers in several countries. Further, the use of brute force, such as cargo truck hijackings, is also on the rise, particularly in South Africa. BSI found that hijackings increased by nearly 25% in the first half of 2021.

Disruptions and rising costs, in part due to criminal activity, will continue to have a negative impact on the supply of goods. Shortages of food, electronics and fuel will persist, providing additional opportunities for bad actors to insert themselves into the economy by selling counterfeit goods at a markup and laundering the profits this generates.



The illicit drug trade is also evolving. As quarantines and lockdowns are introduced and lifted in different parts of the world, drug cartels are diversifying their trade routes and modes of transport. For example, while the BSI found that cocaine seizures in Europe increased in 2021 — a trend that the BSI expects to continue into 2022 — where these seizures have occurred is also notable. Traditionally, ports in Belgium and the Netherlands have recorded the most shipments stopped from criminal organizations in Ecuador, Brazil and Columbia. But in 2021, authorities seized several large shipments of cocaine from these countries at ports in Ireland, France, Montenegro and Greece.

Authorities have noted an increase in drug seizures in the US, too, with a 90% rise in November 2021 compared to the month before — due, in part, to easing travel restrictions. Along with cocaine, transnational crime syndicates, primarily from Mexico, export massive amounts of methamphetamine, marijuana, fentanyl and heroin into the US each year. Typical smuggling techniques include bulk transport and the use of commercial and passenger vehicles, commercial cargo trains, passenger buses, and maritime vessels, small aircraft and couriers and underground cross-border tunnels. Billions of dollars in proceeds — anywhere from $19 to $29 billion — then flow back into the pockets of Mexico's drug cartels.

Detection of these illicit money flows requires particular vigilance from financial institutions located near the US-Mexico border or in critical drug trafficking areas. Even so, all financial institutions in the US should remain on high alert. Drug traffickers tend to use a variety of methods to move funds in and out of the country, including wire transfers, shell and legitimate business accounts, funnel accounts and structured deposits with money remitters.

What does this mean for my business?

Firms should continue to carry out sanctions and adverse media checks on their customers. They should also ensure that they perform Know Your Business (KYB) checks, particularly when dealing with firms operating in supply and logistics, to ensure that they are legitimate businesses. Banks that have trade finance products should carry out transactional due diligence to understand all parties to a transaction.

The Rising Threat of Fraud

Fraud will remain a focus for financial institutions and governments alike, especially as societies continue to grapple with COVID-19. In 2020 and 2021, as a result of the pandemic, countries rushed to implement stimulus packages and provide monetary assistance in the form of extended welfare programs, government-backed loans and other measures. That inevitably created ample opportunities for exploitation, which will continue into 2022. When asked about the predicate offenses they are screening against (Figure 4), there was a notable drop in concern about fraud — 61% cited this in 2020, compared to 37% in 2021. However, despite this marked decrease, it remains one of the top three predicate offenses firms are concerned with.

The losses linked to either fraud or loan defaults will total several billion dollars. Initial estimates indicate the UK, for example, could see losses of up to £26 billion on COVID-19 business loans. The US has already identified a total of $84 billion in suspected fraud linked to COVID-19 stimulus packages, and the EU's fraud chief has warned that the bloc's €800 billion pandemic recovery fund is at risk.

A good portion of the funds obtained illicitly will flow through the financial system via traditional methods; however, the use of money mules and money mule networks to launder funds is a typology that firms should pay close attention to with respect to detecting fraud. In addition, it's important to consider how new technologies can alter the red flags associated with traditional typologies. Virtual currencies, for instance, are becoming more mainstream, and the anonymity inherent in many cryptocurrency transactions makes it an attractive method to quickly and easily launder funds. Therefore, it's likely to become more common for money mules to convert funds from welfare or stimulus payments to a form of cryptocurrency as part of the laundering process.

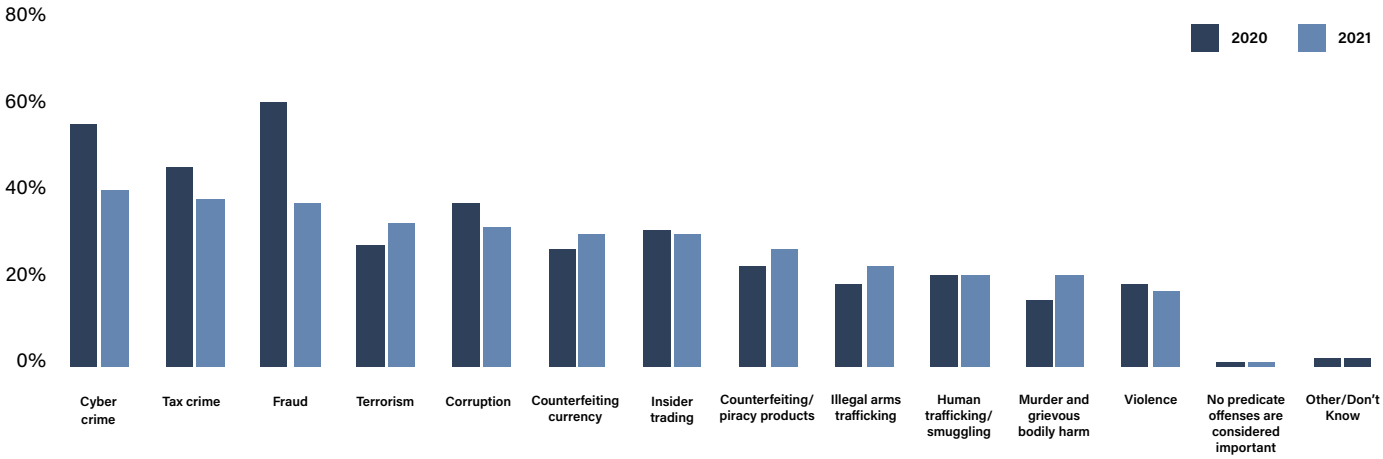
More generally, the continued digitization of the financial system will alter the fraud landscape. As digital wallets and contactless payments build further momentum, the digital payments market is expected to reach $10.7 trillion by 2025, up from an estimated $6.8 trillion in 2021. Reports of e-fraud and the misuse of electronic payment networks and e-money are expected to increase. The UK has already confirmed 71% jump in authorized push payment fraud during the first half of 2021, a scheme in which customers are tricked into sending money to accounts controlled by scammers.

Such scams will continue. Criminals may also use techniques such as remote access trojans, e-skimming malware, auto-dialers, phishing as a service (PhaaS) subscription models, phishing, payment diversion fraud, CEO fraud, business email compromise schemes, invoice redirection, salary diversion and account takeover fraud.

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

Figure 4

'ComplyAdvantage: The State of Financial Crime 2022'



What does this mean for my business?

Firms should fine-tune their transaction monitoring systems to ensure that they take into account fraud methods across various payment chains and that they can detect the laundering of funds defrauded from stimulus packages. As in the 2020 survey, the top AML tools organizations are planning to replace or upgrade in 2022 relate to transaction monitoring. Firms should also invest in awareness campaigns for their employees and customers to raise knowledge of the pitfalls of fraud and how to detect and prevent fraud from occurring.

Ransomware

Ransomware attacks have proven to be a low-cost, high-return method for extorting funds from individuals and businesses alike.

Many of the targets have been high-profile, such as the attack that hit the Metropolitan Police Department in Washington, DC, in April 2021 and the two carried out against Colonial Pipeline and the global beef manufacturer, JBS, the following month. In May, four subsidiaries of an insurance company in Thailand, Malaysia, Hong Kong and the Philippines were hit with a $20 million ransomware attack. In July, the cybercrime group REvil attacked the software provider Kaseya, hijacked the systems of over 200 companies, and demanded over $70 million in bitcoin in return for decryption keys — the largest ransom to date. In September, a Malaysian web-hosting service was targeted by a ransomware attack in which a $900,000 payment was demanded in cryptocurrency. Thailand has also seen computer systems in its hospitals and companies encrypted and blocked.

Further, while some entities, such as the Metropolitan Police Department, have refused to pay the ransom — a decision that resulted in the release of sensitive departmental data — others have capitulated to the hackers' demands. Colonial Pipeline, for example, paid $4.4 million. Just over half ($2.3 million) was recovered a month later.

These high-profile cases highlight a growing problem. Over 304 million attacks were reported worldwide during the first half of the year. That is equal to the number of attacks that occurred throughout all of 2020. The United Nations Office on Drugs and Crime (UNODC) noted that the digitization of society, alongside the pandemic, had contributed to a 600% rise in cybercrimes in Southeast Asia. It noted that ransomware in particular has "skyrocketed" and is now the most prominent malware threat.

There will continue to be an explosion of ransomware activity in 2022. By 2031, research firm Cybersecurity Ventures predicts that there will be a new attack every two seconds, with damages costing the world $265 billion. Targets remain varied and include hospitals, banks, critical infrastructure, educational institutions and financial institutions.

The rising frequency and severity of ransomware attacks prompted the Financial Crimes Enforcement Network (FinCEN) to issue an advisory, published in November 2021, that details new trends and typologies. Among other insights, the US financial intelligence unit noted that cybercriminals often use wide-scale phishing and targeted spear-phishing campaigns. These prompt individuals to download malicious software, exploit remote desktop protocols and software vulnerabilities, and host malicious code on otherwise legitimate websites.

In addition, ransom payments are frequently requested in cryptocurrencies. While Bitcoin is still the most common currency, requests to pay the ransom in anonymity-enhanced cryptocurrencies such as Monero are increasing. The payments themselves typically involve different wallet addresses and, increasingly, the use of mixers to make it harder for authorities to trace the transactions. This money laundering strategy mixes the illicit funds with other funds belonging to other users before splitting the total value into smaller chunks that pass through several intermediary steps before arriving at a final destination. Often, criminals use foreign exchanges in high-risk jurisdictions with lax compliance controls or regulatory oversight to cash out and convert the funds to fiat currency.

Other regulatory bodies are also taking note, and financial institutions should be aware that they may wittingly or unwittingly be liable for potential sanctions violations if they facilitate ransomware payments. The US Office of Foreign Assets Control, for example, issued an advisory in October 2021 highlighting those sanctions risks and reminding institutions under its jurisdiction that it has already designated several entities involved in ransomware attacks.

What does this mean for my business?

It is essential that firms boost their cyber defenses and practice cyber hygiene. They must have strong cybersecurity controls and have implemented business continuity and resiliency plans. Firms should also familiarize themselves with the typologies identified by FinCEN and build these into their controls. Finally, they should make their employees aware of the sanctions risks of processing payments on behalf of victims.

Crypto, NFTs and DeFi

The year 2021 was a turning point for digital assets such as cryptocurrencies and non-fungible tokens (NFTs).

The cryptocurrency market reached an all-time high in November 2021, briefly hitting a market cap of $3 trillion. Its cap fell to around $2.33 trillion toward the end of 2021. Nevertheless, this still represents a significant leap from November 2020, when it was worth $578 billion, and the market is expected to continue to grow.

Similarly, NFTs as an asset class experienced significant growth, with individuals sending nearly $27 billion in cryptocurrency to the smart contracts linked to NFTs from January to October. Yet, while the majority of NFT transactions have been driven by retail investors and users so far, there is evidence that NFTs are gaining in value and attracting attention from major investors. In March, an NFT of the digital artist Beeple's artwork sold for over $69 million at Christie's. Then, Sotheby's hosted a digital art auction in June featuring the popular Cryptopunk collection in which 28 lots sold for $17.1 million collectively. All 28 lots had starting bids of just $100. NFTs could reach a total market size of $300 billion by 2030, according to one estimate by Morgan Stanley, with $56 billion of that in the luxury goods industry.

The growth of digital currencies and NFTs signal a wider shift within the financial space toward DeFi, or decentralized finance, which has emerged as an alternative peer-to-peer financial system that relies on smart contracts to execute transactions. Users can access products such as derivatives trading, lending, insurance, asset management, etc. — all without using traditional banking intermediaries. DeFi has also led to the development of new financial services, including margin trading, yield farming, liquidity mining and crypto staking. While still relatively new, the concept of decentralized finance is picking up steam quickly — the DeFi services market grew 1,700% to $247 billion within 2021.

In 2022, all three of these markets will continue to evolve, with adoption likely to increase rapidly. That growth will invite more regulation, not least because criminal activity and exploitation of these markets will also increase. Reflecting the ongoing growth and diversification of the crypto space, firms told us that the crypto-related regulatory development they're most concerned about is transaction monitoring (Figure 5).

Which of the following crypto-related regulatory developments most concerns your organization?

'ComplyAdvantage: The State of Financial Crime 2022'

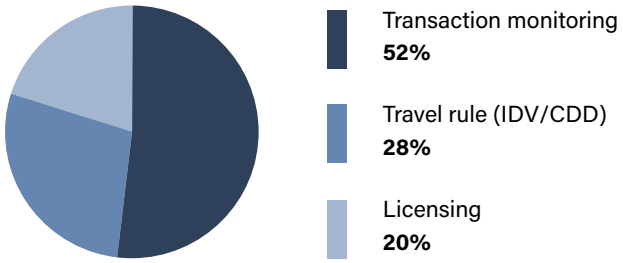


Figure 5

Indeed, many have raised concerns over how criminals can exploit new asset classes and technologies. One study estimates, for example, that 1% of cryptocurrency transactions are linked to criminal activity. That may seem a trivial amount on the surface, but as at least one report points out, given a market capitalization of nearly $3 trillion, 1% amounts to around $20 billion. In the US alone, the IRS seized $3.5 billion linked to fraud cases involving cryptocurrency during the fiscal year 2021. However, as DeFi and NFTs become targets, cryptocurrency hacks and fraud will decrease.

The NFT market is particularly vulnerable. The purchase and sale of art have long been acknowledged to be attractive vehicles for money laundering. Trading NFTs may provide criminals with another avenue to obscure the origin of funds obtained by illicit means, especially given that NFTs aren't subject to regulation unless a marketplace has been created. Monkey Kingdom, a Hong Kong-based NFT project supported by celebrities including JJ Lin and Steve Aoki, was hacked via a Discord group chat, leading to the theft of $1.3 million in cryptocurrency.

Zooming out to examine the overall DeFi system reveals several security gaps. DeFi fraud and theft losses totaled $10.5 billion in 2021, and there have been several notable hacks. In March, $180 million was stolen from PAID Network. Then, in August, a hacker stole $600 million worth of cryptocurrency from the Poly Network. Losses are only expected to increase in 2022. DeFi systems have also been exploited to launder the proceeds of crime through decentralized exchanges (DEXs), decentralized miners and cross-chain bridges.

Pandora Papers and Congo Hold-Up Expose Corruption

The release of the Pandora Papers, which began in October 2021, shed light on the role of offshore corporate structures in obscuring the source of funds from money laundering schemes and facilitating the acquisition of real estate. The nearly 12 million leaked documents exposed the secret offshore accounts and dealings of over 300 prominent world leaders, politicians and other politically exposed persons (PEPs), as well as dozens of influential business leaders and celebrities.

While not all individuals named have engaged in illicit activity, the leak revealed how a considerable number of high-profile individuals had been able to hide their wealth and evade taxes via offshore accounts, shell companies and real estate investments. A few notable revelations include:

- The Qatari ruling family bought two of the most expensive properties in London through offshore accounts, which enabled them to avoid over $25 million in taxes
- King Abdullah of Jordan quietly purchased 15 homes in Malibu, London and Ascot, among other places, totaling over $100 million
- The (now former) Czech prime minister did not disclose the existence of an offshore company through which two French villas worth over $16 million collectively were purchased

The 2021 survey showed compliance teams are closely monitoring many areas of their programs relevant to the Pandora Papers leak. When asked which areas of their AML programs firms are most focused on improving in 2022 (Figure 6), the detection of PEPs and relatives and close associates (RCAs) was top of mind for 48%, followed by virtual asset risk monitoring (46%) and ultimate beneficial ownership (44%).

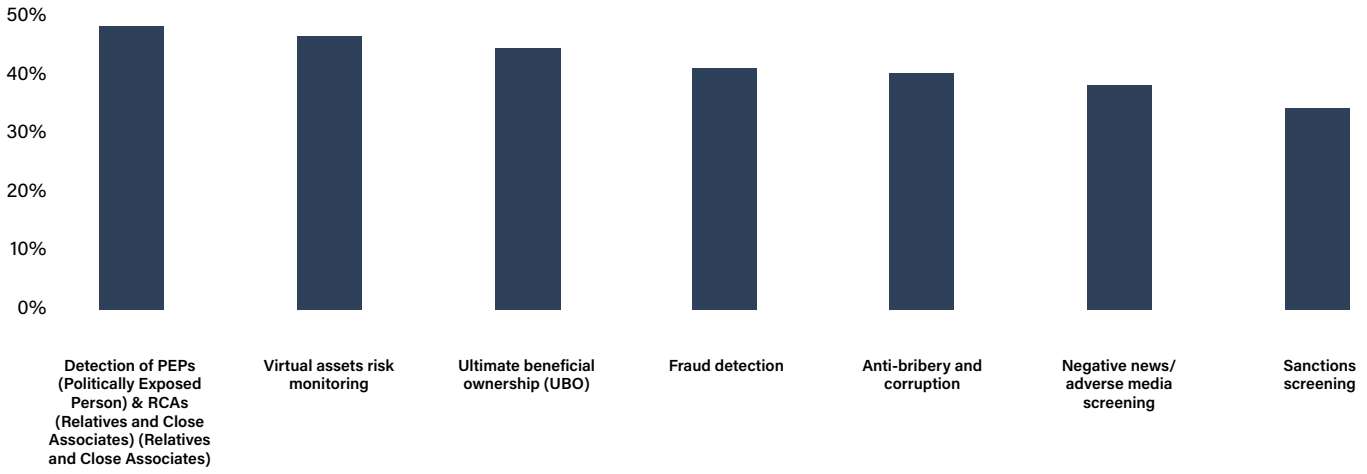
What does this mean for my business?

Increase awareness of the risks and opportunities of blockchain-based transactions. Firms should understand their exposure to emerging financial services and asset classes. Where possible, firms should invest in blockchain monitoring software and adopt appropriate AML/CFT risk mitigation policies and controls. Learn more about reducing risks with real-time screening and automated monitoring.

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

Figure 6

'ComplyAdvantage: The State of Financial Crime 2022'



In addition, the Congo Hold-Up, which broke just a month later, in November 2021, is composed of over 3.5 million documents from BGFIBank — the largest leak of financial data in Africa. These records exposed how the bank, along with its global network of correspondent banks, was used to facilitate the vast transfer of cash abroad. Transactions include alleged bribery payments to the ruling elite of the Democratic Republic of Congo (DRC), real estate investments in multiple countries and a deal in which the DRC's mineral wealth was exchanged for infrastructure investment from China.

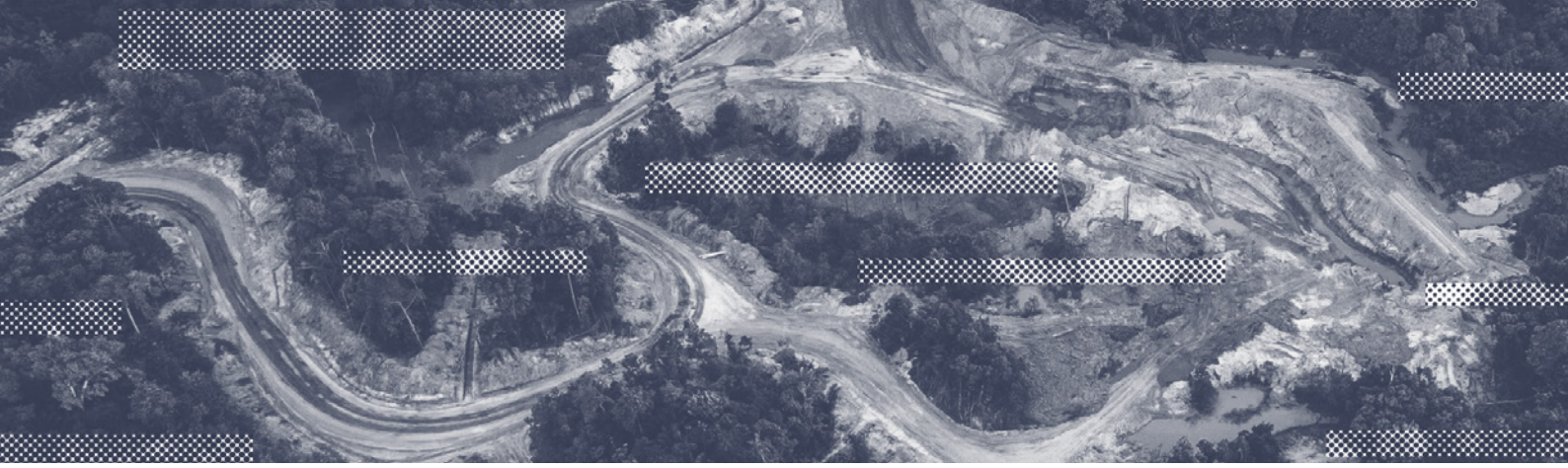
While investigations are ongoing, and the extent of the fallout is unlikely to be understood for some time, these two massive leaks will significantly shape the financial crime and regulatory landscape in 2022. Firms should expect an increased focus on PEPs, tax evasion and tax crimes, as well as the need to understand transnational flows and foreign ownership of real estate investments.

Environmental Crime

Environmental crime has risen in prominence, and several international organizations and intergovernmental bodies have urged action. Notably, in June 2020, the FATF published a report on the illegal wildlife trade in which it urged member states to strengthen environmental crime laws. The FATF issued a follow-up report in July 2021 that offers insights and policy recommendations. In addition, the EU's 6th Anti-Money Laundering Directive (6AMLD), which established environmental crime as one of 22 predicate offenses to money laundering, came into effect in December 2020. Compliance teams under the EU's jurisdiction have had to implement controls that can effectively detect and identify suspicious transactions linked to environmental crime.

What does this mean for my business?

Firms should ensure that they understand the source of funds and source of wealth when dealing with PEPs and companies (especially those based offshore) beneficially owned by PEPs, associates and members of their families. The key to identifying high-risk PEPs is carrying out PEP and adverse media screening.



This global problem is estimated to generate anywhere from $110 to $281 billion in criminal proceeds each year. Examples of environmental (or "green") crimes include:

- Illegal, unreported, and unregulated (IUU) fishing and over-fishing
- Illegal logging
- Illegal mining
- Illegal wildlife trade
- Illegal movement and disposal of waste and hazardous substances
- Pollution
- Waste disposal without a license, including e-waste
- Fraudulent carbon trading

In addition, environmental crime and other criminal activity are closely linked, with the proceeds of the former lining the pockets of transnational crime syndicates, drug, arms, and sex traffickers and terrorist organizations, among others. In fact, a report published by the Global Initiative Against Transnational Organized Crime found that environmental crime "has become the largest financial driver of conflict," with the proceeds accounting for 38% of money spent to fund conflicts and non-state armed groups. It also makes up 28% of financing for drug trafficking and 26% for illegal taxation, extortion, confiscation and looting.

As awareness around environmental crimes grows, we will uncover more money laundering schemes and typologies that link back to these types of crimes. In addition to the more traditional green crimes, financial institutions would do well to learn about emerging green crimes. These include greenwashing — or the fraudulent misreporting of environmental, social and governance (ESG) information, the exploitation of green finance initiatives and fraud linked to green bonds — and the mining of natural resources essential to the growing electric vehicle market.

What does this mean for my business?

Firms should incorporate environmental crime into their business-wide risk assessments and identify countries, categories of customers, industries, products and delivery channels more at risk of being used to facilitate this type of crime. Firms should invest in educating their employees on what environmental crime looks like to help them more easily identify these crimes where they may not initially be apparent. Sources such as adverse media screening and import/export data should also be consulted to identify suspicious activity.

Terrorism and Terrorist Financing

The terrorist threat landscape is evolving. The US will continue to see a rise in polarization, extremist ideologies and violence from across the political spectrum. Authorities have noted that far-right terrorism, in particular — perpetrated by anti-government extremists, white supremacists and anti-abortionists — poses a significant threat. Across the Atlantic Ocean, Europe will grapple with lone-wolf terrorist attacks carried out with simple weapons (vehicles, knives, etc.) and linked to Islamic extremism, as well as left- and right-wing extremism, anarchist organizations and ethnonationalism. In both cases, such threats deviate from traditional terrorist organization networks, tend to be decentralized and rely heavily on social media to share propaganda. Identifying funding streams, therefore, will prove to be challenging.

In Africa and the Middle East, terrorist groups have expanded their influence, taking advantage of power vacuums created by widespread corruption, government oppression and regional instability. The US withdrawal and the subsequent Taliban takeover of many major cities in Afghanistan exacerbated matters, increasing the likelihood of more violence. In addition to the Taliban, groups such as Boko Haram, ISIS, al-Shabab and al-Qaida will continue to carry out attacks and wield control over the regions. Al-Qaida and ISIS's influence extends to Southeast Asia, where the Philippines, Indonesia and Malaysia are especially vulnerable to terrorist attacks. Finally, an uptick in right-wing extremism in Singapore may further destabilize the region.

Terrorist financing efforts have increasingly incorporated new technologies. In recent years, there has been a move to online transfer methods, digital payments, mobile banking and cryptocurrency assets to raise and quickly transfer funds across borders. That will continue in 2022. In addition, terrorists have started to embrace gaming platforms to communicate. More terrorists and terrorist organizations are likely to turn to these platforms and currencies to fund their activities.

Data relevancy — specifically, data being stored in the right categories — is now firms' biggest pain point related to data (Figure 7). In 2020, firms told us coverage — collecting and compelling data globally — was their biggest concern. The speed at which terrorist activities are evolving and adopting new platforms reflects the growing challenge of keeping data sources up to date and, therefore, accurate.

What is your organization's biggest pain point with respect to data?

'ComplyAdvantage: The State of Financial Crime 2022'

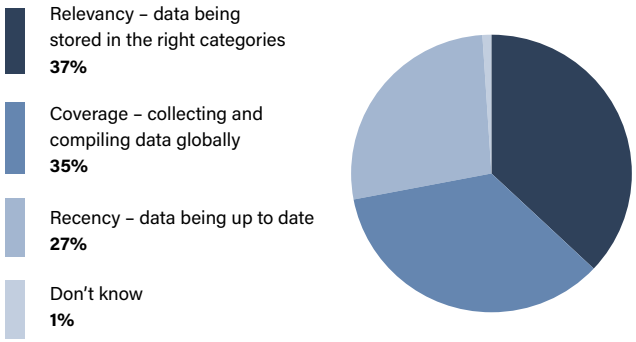


Figure 7

What does this mean for my business?

Firms should regularly screen against sanctions designations. They should also understand how terrorist financing takes place in different regions. National risk assessment documents should be reviewed to identify terrorist financing methods, and payments going to jurisdictions with high terrorist financing activity should be scrutinized. To guard against the de-risking of not-for-profit organizations, firms should ensure they understand how funds are raised and distributed and the control environment in different not-for-profit organizations.

Geopolitics and **Sanctions**

2022 will see countries contend with a rapidly changing, varied and tense geopolitical landscape.

Relations between the West, Russia and China will remain strained. The November 2020 G20 Summit provided early evidence of this, with both countries not attending in person. Environmental crime, corruption and AML/CFT measures were discussed.

The potential for new coronavirus variants, economic uncertainty and political crises such as human rights abuses and coups in hotspots around the world could push geopolitical tensions to a breaking point. Particular attention should be given to ongoing tensions in Afghanistan, Cuba, Ethiopia, North Korea (DPRK), Myanmar, Sudan, Hong Kong, Ukraine and Iran.

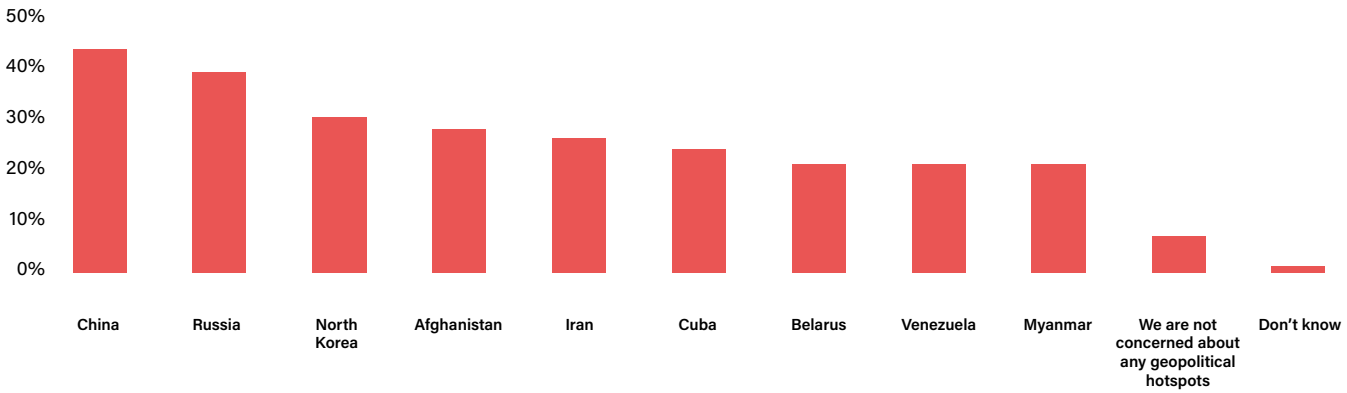
This fractious global picture could allow for the rise of illicit financial flows, as criminals rebuild and exploit fragile states, conflict zones, power vacuums and the mistrust that exists between countries. The propensity for sanctions and trade restrictions to be implemented at short notice has elevated further the importance of real-time risk data. 96% of firms said real-time AML risk data would improve their compliance operations. The number saying it would improve operations "significantly" increased by 15 percentage points in 2021, compared to 2020.

The West vs China

Following high-profile confrontations with the United States, Australia and others, alongside its integral significance to the global economy, it's unsurprising that China is the top geopolitical hotspot firms are most concerned about heading into 2022 (Figure 8).

Which of the following geopolitical hotspots is your organization most concerned about? *Figure 8*

'ComplyAdvantage: The State of Financial Crime 2022'



Xinjiang Uyghur Autonomous Region

In Xinjiang, the UN has been leading international scrutiny related to the detention of Uyghurs and other Muslim minority groups. There are also concerns about forced labor, with workers in the province being transferred to factories. At the time of writing, the United Nations' human rights office was finalizing a report assessing the situation in more detail.

Ongoing concern about human rights abuses in Hong Kong and Xinjiang, alongside what the UK's Foreign Secretary has termed "coercive economic policies" may lead to the use of additional Global Magnitsky-style sanctions against China. Additional trade sanctions to manage concerns around the use of technology to advance China's military are also possible. These measures would build on a host of activity through 2021, including coordinated international sanctions in March 2021 and additional sanctions issued by the US in December.

The latter measures banned all imports from Xinjiang in response to concerns about the Uyghur Forced Labor Prevention Act. As the region produces almost 90% of China's cotton, these measures will have a significant impact on the fashion industry. Sanctions were also issued on eight firms, including the world's largest drone manufacturer, and a company using facial recognition technology to track minority groups and alert officials if too many individuals gather in specific locations. In a separate notice, the US Commerce Department restricted sensitive exports to 11 research institutes linked to the Academy of Military Sciences due to biotechnology work, including "purported brain-control weaponry."

In another sign that the long-running dispute will continue well into 2022, countries including Australia, Canada, the US and the UK have also pledged a diplomatic boycott of the Beijing Winter Olympics over Xinjiang.

It's likely that much of the focus will remain on Communist Chinese Military Companies (CMMCs), with the potential for additional sanctions from the US. So far, the US has released several tranches of sanctions, including against CCMCs such as SenseTime, which had been due to issue its IPO, alongside other Chinese biotech and surveillance companies. China has indicated it will "strike back" for "perverse actions" on the part of the US.

On June 3, 2021, the US issued Executive Order (EO) 14032 entitled 'Addressing the Threat From Securities Investments That Finance Certain Companies of the People's Republic of China', which replaced previous EOs on CCMCs. It maps out how the US views the threat posed by China to its national security, including:

- Involvement in the research of military, intelligence, security and development programs, as well as weapons and related equipment produced under China's military-civil fusion strategy
- The use of Chinese surveillance technology outside of China and the development/use of surveillance technology to repress people or commit human rights abuses

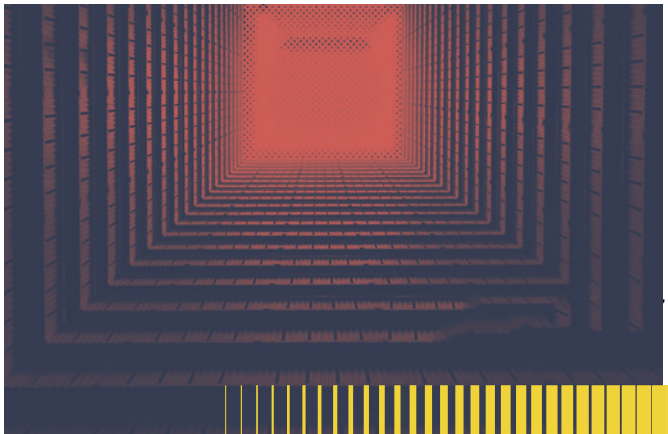
EO 14032 also provides a list of CCMCs that are under sanctions measures and extends these to their owners and controllers.

However, the adoption by China of its "Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures" (Blocking Statute), enacted in January 2021, may limit the impact of US sanctions and the extraterritorial reach of US sanctions in China in 2022. The rules empower MOFCOM, China's Commerce Ministry, to act when laws and regulations from other countries impact "normal economic, trade and related activities."

Hong Kong

In Hong Kong, China continues to exert its influence. The latest sign of this came with the closure of major pro-democracy news outlets through 2021. In June 2021, Apple Daily, a popular pro-democracy tabloid, closed its doors. At the end of 2021, the region's biggest remaining pro-democracy news outlet, Stand News, was closed after being targeted with a national security investigation.

In July 2021, the US federal government released a business advisory on "The Risks and Considerations for Businesses Operating in Hong Kong." The advisory highlights growing risks for US companies operating in Hong Kong related to national security, data privacy, transparency and the particular risks for businesses exposed to sanctioned Chinese entities. In the same month, the US sanctioned seven Chinese officials over what it termed the erosion of the rule of law in Hong Kong.



The Chinese government has delayed directly imposing the Anti-Foreign Sanctions Law (AFSL) in Hong Kong — a move that would have allowed the Chinese government to seize assets from entities that implement US sanctions. Building on the rules published in January, the AFSL empowers Chinese authorities with a number of counter-sanctions, including blocking assets and transactions, as well as visa restrictions.

The AFSL is likely to remain a geopolitical flashpoint in 2022. A top adviser to Carrie Lam, Hong Kong's chief executive, has said the adoption of a local version is likely. It remains unclear whether the law would be added to Hong Kong's Basic Law or imposed directly from Beijing, in line with some national security actions. The uncertainty is contributing to a fractious and uncertain environment for financial firms in the region.

Even if the AFSL were to be imposed on Hong Kong, it's unclear how disruptive it would be. Despite the broad scope of the legislation, when it was introduced in China, no senior Biden administration figures or US companies were targeted. The first wave of counter-sanctions introduced under the law targeted seven American individuals and entities, including Wilbur Ross, former President Trump's commerce secretary. Rather, extending the AFSL to Hong Kong may primarily be designed to give China additional leverage in its ongoing trade disputes with the US, given the importance of the region as a financial center to the global economy.

Taiwan

With China focused on maintaining its COVID-Zero strategy, delivering the Winter Olympics and managing its economy, Taiwan is unlikely to become militarized in 2022. However, President Biden's decision to make a meeting of the so-called "Quad" representing Australia, Japan, India and China one of his first summits upon taking office demonstrates the sensitivity, uncertainty and high-profile nature of the situation.

Lower-level tensions will continue. In November 2021, China sanctioned Taiwan's premier, foreign minister, parliamentary speaker and their relatives, prohibiting them from entering China. Companies linked to sanctioned persons will also not be allowed to make profits in China. China has also said it is compiling a "global watch list" of Taiwanese independence backers.

China will continue to exert economic and diplomatic pressure on countries it views to be overly supportive of Taiwan. Lithuania's decision to open a Taiwanese representative office in its capital — the first time an EU member state had let Taiwan use its own name for a foreign outpost — led to China downgrading its diplomatic relations and restricting trade.

US-China relations

Despite US-China relations being described by Secretary of State Anthony Blinken as "the biggest geopolitical test of the 21st century," the trade war between the two countries shows no signs of abetting, with both countries likely to continue applying "tit-for-tat" sanctions. Expectations that both sides would look to de-escalate the situation have been dashed by continued US pressure on Xinjiang and other measures viewed by China as aggressive.

The G7 summit in June 2021 also saw the launch of the $40 billion Build Back Better World (B3W) program. Widely viewed as a response to China's Belt and Road Initiative (BRI), B3W is designed to promote good governance, transparency and human rights alongside economic investment. It's likely to include a due diligence component and a requirement to mitigate the risk of corruption and human rights abuses.

As additional details on the scope, goals and funding mechanisms of B3W emerge in 2022, firms will gain a clearer understanding of the key areas of overlap and divergence with China's BRI. It's already clear that the two programs will have different focus areas. While BRI funds "hard infrastructure" such as ports, roads and railways, B3W is designed to focus on "softer outcomes," including health security and modernized digital technology. Although China has renewed claims to develop the "Health Silk Road," "Digital Silk Road" and "Green Silk Road," analysts note it remains primarily focused on traditional BRI projects.

B3W also aims to mobilize funding through private capital, alongside development institutions, bilateral partnerships, multilateral development banks and other financial institutions. It's unclear, however, if/how institutions such as the Export-Import Bank of the United States will contribute to rolling out B3W.

A virtual summit between Presidents Biden and Xi in November 2021 was labeled a photo opportunity by some commentators. But both sides did agree not to escalate their dispute further. The US has since announced a diplomatic boycott of the 2022 Winter Olympics in Beijing, where China's central bank digital currency (CBDC) will be launched.

Cybersecurity is likely to be another area where tensions escalate in 2022, with analysts expecting tighter restrictions on the export of critical technologies to China. Measures could include export controls, the screening of outbound investment to China and the closing of regulatory loopholes, including, for example, one that currently allows Chinese semiconductor maker SMIC to continue purchasing critical US technology.

The US is likely to continue to balance issuing new sanctions against China with attempts to stabilize relations. Expect any new sanctions to focus on human rights violations, cyberattacks, violations of international law and state sovereignty. The UK also recently added China to its list of countries subject to military end-use controls.

China-Australia relations

2022 is also unlikely to bring the normalization of relations between Australia and China, especially in the run-up to federal elections in Australia due in the summer. The relationship became strained in 2020 when Australia condemned China's human rights record and endorsed an investigation into the origins of COVID-19. China retaliated with an 80.5% tariff on barley exports, frustrating Australian coal exports, imposing tariffs from 107% to 212% on wine and unofficially banning beef, lobster, timber, sugar and copper.

In 2021, relations continued to worsen, with Australia canceling two BRI deals and China announcing the suspension of the China-Australia Strategic Economic Dialogue. Australia also joined the US' boycott of the Beijing Winter Olympics over human rights abuses in Xinjiang.

China also responded with fury to the AUKUS partnership. Announced in September 2021, the partnership is designed to help Australia acquire a fleet of nuclear-powered submarines to counter China's influence in the Indo-Pacific. China has argued the pact is a violation of the 1985 Rarotonga Treaty, which makes the South Pacific a nuclear weapons-free zone. Attempts to build a consensus in the region either for or against the partnership are unlikely. In New Zealand, for example, national law prohibits the country from allowing Australia's nuclear-powered submarines in its ports, but Prime Minister Jacinda Ardern said she was "pleased to see" AUKUS. The pact remains a potential geopolitical flashpoint, however, as the collision of a US submarine with an "unknown object" while in international waters in the South China Sea demonstrated.

What does this mean for my firm?

Firms should monitor US-Chinese relations closely, particularly as the Winter Olympics approach, alongside the launch of China's CBDC. Robust sanctions screening and transaction monitoring systems should be in place to identify human rights abusers swiftly, as well as any transactions that may breach sanctions.

US Summit for Democracy

Launched as part of President Biden's campaign pledge to tackle corruption, the US Summit for Democracy will continue to provide an avenue for governments to launch initiatives around transparency, beneficial ownership, asset tracing and recovery, and the transparency of real estate transactions.

On June 3, 2021, corruption was identified as a core US national security interest, meaning the federal government will continue to focus on:

- Supporting democracy at home and abroad and defending against authoritarianism
- Addressing and fighting corruption, including illicit financial flows
- Promoting respect for human rights and open societies
- Defending media freedom and protecting journalists
- The responsible use of technology

The US also released its "Strategy on Countering Corruption" a whole-of-government strategy to support the fight against illicit finance more effectively, hold corrupt actors to account and strengthen the capacity of those exposing corruption, including activists, journalists and civil society.

The strategy includes a particular focus on sanctions measures, such as:

- The launch of Democracies Against Safe Havens (DASH) to boost international cooperation
- A new team in the US Treasury to support corruption sanctions
- A commitment to continuing an ongoing review of risks linked to digital assets, including sanctions evasion
- Indicated ongoing support for corruption reporting and submission by civil society

What does this mean for my firm?

Firms operating in the US or with a US nexus should ensure that they stay on top of a rapidly changing landscape, including by conducting horizon-planning and remaining on top of changing laws, regulations and initiatives. Firms will need to assess legal and regulatory changes and any new initiatives that may need to be incorporated into policies and processes, including onboarding and transaction monitoring, but also as part of a firm's anti-bribery and corruption programs.

Russian Ambitions: Ukraine and Nord Stream 2

Ukraine

Russia's geopolitical ambitions and the EU's dependency on Russia for its energy needs mean governments will need to strike a balance between national security, economic interests and the use of sanctions.

The ongoing Ukraine crisis is a clear example of this. If Russia escalates the situation further, the use of coordinated sanctions is highly likely. By late 2021, almost 100,000 Russian troops have amassed at the Ukrainian border, with concerns that an invasion is imminent. This could manifest as a direct conflict or as a "hybrid war" built around information campaigns and cyberattacks on systems and infrastructure.

G7 countries issued a statement condemning the Russian military build-up and arguing that "military aggression against Ukraine would have massive consequences and severe cost in response." The EU has stated that certain actions would trigger "high impact" sanctions. Russia has denied it intends to attack Ukraine.

Nord Stream 2

Nord Stream 2, the contentious $11 billion pipeline under the Balkan Sea built to carry gas from Russia into Germany while bypassing Ukraine, remains a concern for the US. The US is likely to continue imposing new sanctions when it is in the country's national interest to do so, but may waive them in certain circumstances. For example, in 2021, measures were lifted against Nord Stream 2 AG and its chief executive, Matthias Warnig.

Nord Stream 2 sanctions have been imposed under the Countering America's Adversaries Through Sanctions Act (CAATSA). Guidance on section 232 of CAATSA was recently updated so that it now appears to cover any US person involved in financing Nord Stream 2. Those covered include persons who:

- "Make investments that directly and significantly contribute to the enhancement of the ability of Russia to construct energy export pipelines; or
- Sell, lease or provide goods, services, technology, information or support to the Russian Federation for the construction of Russian energy export pipelines"

"Significant investments" are set at a minimum of $1 million, or $5 million over a 12-month period, while "investments" are defined as "a commitment or contribution of funds or other assets or a loan or other extension of credit to an enterprise."

However, the EU stated in November 2021 that it does not recognize the anti-territorial nature of sanctions issued by the US Office of Foreign Assets Control (OFAC), and will not impose sanctions on companies that are complying with EU law. Germany has said it will impose sanctions if Russia uses the provision of energy as a weapon or attacks Ukraine. If this were to happen, retaliatory sanctions from Russia should be expected.

Kazakhstan

Russia will continue its involvement in the evolving situation in Kazakhstan, following the eruption of widespread protests over the doubling of gas prices. The violence led President Tokayev to request help from the Collective Security Treaty Organization (CSTO), with Russia, Belarus and Armenia sending troops to protect critical infrastructure.

As the world's second largest Bitcoin mining destination, with over 86,000 mining machines, the unrest and energy shortages are causing severe disruption to the industry. Bitcoin mining accounts for 8% of Kazakhstan's energy capacity. As a result, miners have been faced with frozen machines, blackouts, power cuts and internet shutdowns. The Bitcoin network lost 12% of its hashrate, which refers to the amount of computational power used by miners. The protests are estimated to have cost miners in the country around £20 million.

What does this mean for my firm?

Firms should be prepared for any sanctions against Russia by identifying Russian financial exposure and clients on their books to be able to apply any freezing measures should the situation escalate further. Firms should also ensure that they have robust sanctions and adverse media screening systems in place to identify not only designated persons but firms with direct exposure to designated persons and associates.

Political Unrest and Organized Crime

Political unrest and power vacuums have helped organized crime groups to thrive and infiltrate state-run institutions. The 2021 Global Peace Index (GPI) indicates that 2021 was a "year of civil unrest." In particular, the GPI highlighted a 10% "significant increase in civil unrest and political instability" due to COVID-19 restrictions and economic instability, especially in Latin and South America. In total, there were nearly 15,000 demonstrations globally in 2020, with 5,000 of those related to COVID-19.

Meanwhile, the Global Organized Crime Index for 2021 found that 80% of the global population lives in countries with high levels of criminality. Criminals "retooled" their business and exploited opportunities created by the pandemic. People, communities and businesses are also now more vulnerable to organized crime networks, both as victims and potential recruits.

In 2022, organized crime groups will continue to thrive in Latin America, particularly in Mexico, Brazil and Colombia. The region has the world's highest per-capita homicide rate, accounting for one in three of the world's murders. The pandemic has also enabled different criminal organizations to reconfigure how they influence "everyday community dynamics," according to a report in the Georgetown Journal of International Affairs. It's likely that the lines between licit and illicit markets, politics and governance will continue to blur, with groups expanding beyond the drug trade. The report highlights several specific risks:

- The systematic extortion of both formal and informal businesses, leading to the development of high-interest loans where formal credit is scarce
- A wider economic downturn in Latin America could lead to a rise in demand for informal credit lines issued by criminal actors
- Illegal timber logging and exotic wildlife trafficking requires complex arrangements between timber, drug trafficking organizations and sawmills to allow for a mix of illegal and illegal timer sold to firms and other legal sectors of the economy
- A worsening of the pandemic alongside a rise in unemployment risks driving more people to engage in illicit industries in order to provide for their families

Organized crime groups will also continue to meet the needs of local populations where governments are not doing so, helping to strengthen their legitimacy. In Brazil, gangs enforced quarantine policies, while in Mexico, the daughter of infamous drug trafficker El Chapo has been photographed filling boxes with basic goods to distribute to locals.

In December 2021, President Biden issued an executive order establishing a United States Council on Transnational Organized Crime (USCTOC) to develop a coordinated whole-of-government strategy.

What does this mean for my firm?

Adverse media is key to identifying potential links to criminality. Additionally, firms should ensure that their staff are adequately trained on the risks posed, and methods used, by transnational criminal networks and where and how to report suspicions of money laundering.

Thematic and Country Sanctions

US Sanctions Innovation

The US has continued to innovate in the sanctions space, publishing its comprehensive sanctions review in October 2021. The review reiterated the importance of sanctions to the advancement of national security interests. It also identified challenges and risks associated with new payment systems, the use of digital assets, cybercriminals and the need to ensure a flow of legitimate humanitarian need.

Looking ahead, the review highlighted several key priorities for the US sanctions program:

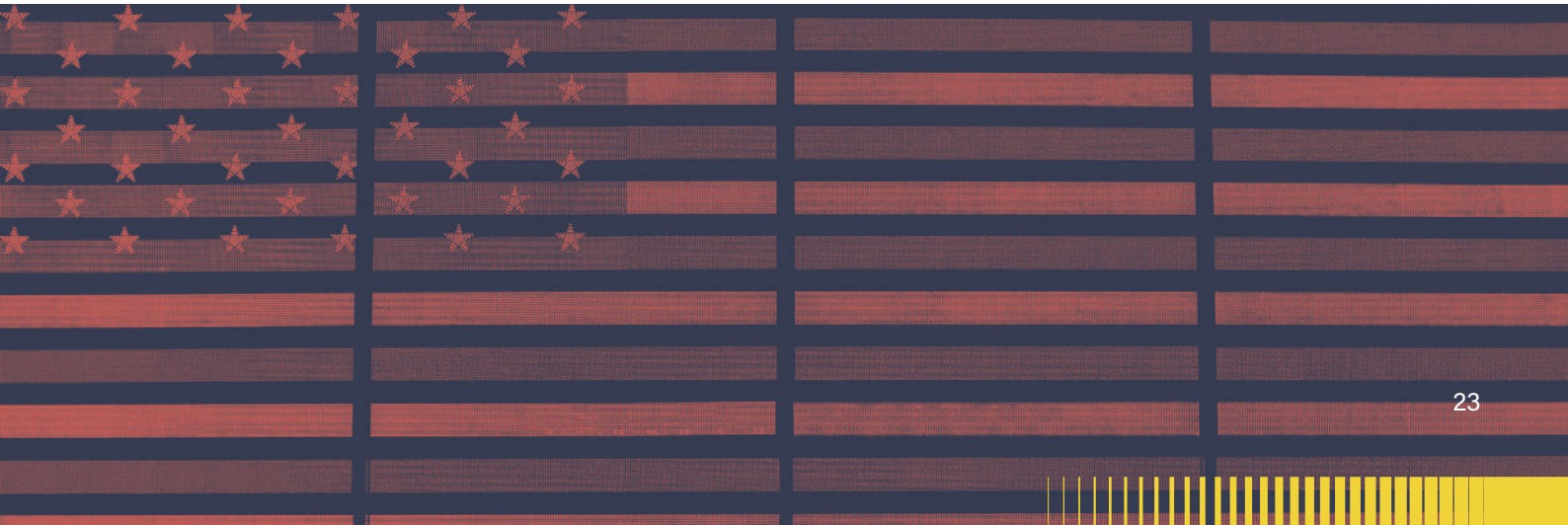
- A multilateral approach to coordinate sanctions with allies and partners
- A structured policy framework linking sanctions to clear policy objectives
- The calibration of sanctions to minimize unintended consequences
- Investment in sanctions technology, workforce and infrastructure
- Ensure sanctions are easily understood, enforceable and reversible

The US will develop new approaches to enable the use of sanctions to target emerging technological and other perceived national security threats.

OFAC also published new sanctions compliance guidance for the virtual currency industry. It provides an overview of the requirements, procedures and best practices firms should follow. This includes an emphasis on cybersecurity alongside the need to monitor IP addresses using geolocation tools. Screening against sanctions lists and carrying out ongoing transaction monitoring are also included.

SUEX, a Russian-based cryptocurrency exchange, became a high-profile target of US sanctions in 2021. On September 21, it was sanctioned for facilitating transactions connected to ransomware, the first time an exchange was designated for this reason. Over 40% of transactions processed by the exchange were linked to illicit actors, laundering proceeds from at least eight separate ransomware attacks.

In December 2021, President Biden signed an executive order (EO) that imposes sanctions on foreign persons involved in the global illicit drug trade. The goal of his EO was to address international drug trafficking, including the growing use of fentanyl, alongside the wider opiate and online drug markets.



The US also imposed a visa ban on wildlife traffickers from the Democratic Republic of Congo (DRC) using section 212(a)(3)(C) of the Immigration and Nationality Act. The ban targets wildlife and timber traffickers who are believed to be, or have been, complicit in or involved with trafficking wildlife, wildlife parts or products.

The Bureau of Industry and Security (BIS) will continue to impose trade sanctions in the cyber and military sectors. BIS also issued FAQs on "cybersecurity items" under its Export Administration Regulators (EAR). The FAQs relate to interim rules issues in October that set out tighter export controls on surveillance tools and dual-use items related to "intrusion software."

BIS has also issued a request for comment on priorities for US-EU export control cooperation — this includes action on advancing the military capabilities of initiatives such as China's quantum development, Pakistan's nuclear program and Iran's military and space programs.

Increased Sanctions Coordination

Throughout 2021 there were repeated examples of like-minded states coordinating the deployment of sanctions in order to maximize their impact. Some of the key examples include:

- December 2021: The UK, US, EU and Canada issued coordinated sanctions for "continuing attacks on human rights and fundamental freedoms in Belarus, disregard for international norms and repeated acts of repression"
- December 2021: The UK, Canada and US also applied sanctions for human rights abuses in Myanmar
- November 2021: US, UK and Canada took action against Nicaraguan officials for human rights abuses following rigged elections
- September 2021: The US and Qatar took coordinated action against Hezbollah
- March 2021: The EU, UK, US and Canada announced coordinated sanctions over human rights abuses in Xinjiang

In particular, the adoption of Global Magnitsky-style (GloMag) human rights sanctions programs will continue. In total, the US has issued 176 GloMag designations, three times as many as in previous years. The US is likely to continue leading the way on both corruption and human rights sanctions programs.

During the US Summit for Democracy week in December 2021, the federal government released new GloMag sanctions every day. We may also see the EU explore adopting an anti-corruption sanctions regime.

On December 2, Australia also passed its Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act covering human rights, corruption and other abuses.

Norway has also introduced a GloMag-style sanctions law to cover human rights abuses, but not corruption.

Regulators Focus on Proliferation Financing Sanctions

In June 2021, the FATF released a proliferation financing risk assessment and supporting guidance. It places an emphasis on countries allowing obliged entities to leverage financial sanctions and compliance programs to mitigate proliferation financing risks. Measures to manage risks include better onboarding of customers and beneficial owners, enhanced due diligence, effective sanctions screening and identifying potential sanctions evasion through the testing of controls.

The FATF also provides a list of risk indicators associated with customer profiles, account or transaction activity, the maritime sector and trade finance. Firms should ensure they are screening against relevant UN sanctions on the proliferation of weapons of mass destruction (WMDs) and its financing — these should have been adopted in national sanctions programs. The key measures to note are:

- UN Resolution 1718 on North Korea (DPRK) and successor resolutions
  - Covers persons or entities engaged in, supporting or who have contributed to the DPRK's nuclear-, WMD- or ballistic missiles-related programs; legal persons or entities directly/indirectly owned, controlled, acting on behalf of a designated person; those who have assisted in the evasion of sanctions; or any entity of the Government of the DPRK or Workers' Party of Korea associated with the DPRK's nuclear or ballistic program

- Further sanctions are possible in the DPRK in relation to UN Security Council Resolutions (UNSC) on the country's provocative actions, nuclear ambitions and WMD/ballistic missile programs. The DPRK is also still holding between 17 and 100 Japanese nationals who were abducted in the 1970s and 1980s, another possible driver of new sanctions

- UN Resolution 2231 on Iran and successor resolutions

  - Covers persons or entities engaged in, providing support for or directly associated with Iran's proliferation of nuclear activities contrary to the Joint Comprehensive Plan of Action (JCPOA) or development of delivery systems including procurement of prohibited items; persons or entities acting on behalf of a designated person; or those who have assisted in the evasion of sanctions or acting inconsistently with JCPOA

  - Negotiations on re-enacting the JCPOA have resumed, with countries calling on Iran to halt its nuclear escalation and make a deal "while this is still possible"

Key Country-Specific Sanctions Programs

Sanctions are targeted at specific countries as a diplomatic and/or financial tool to address crises, perceived violations of international programs, and to target predicate offenses for money laundering.

One area of increased focus has been Eastern Europe and the Western Balkans. Specifically:

- **Belarus**: Sanctions are likely in response to what NATO has called "irregular migration" designed to put political pressure on the EU. The EU is proposing a new legal framework that would allow it to adopt targeted measures that address irregular migration for political means against transport operators (including land, air, inland waterways and sea) as well as those organizing or participating in the "instrumentalization of people." This is defined as actors engaged in or facilitating the smuggling or trafficking of people into the EU. The measures are also designed to address the situation at the border, human trafficking and continued repression in Belarus

- **Bosnia and Herzegovina**: In December the G7 issued a statement condemning "divisive and irresponsible rhetoric and action" and called for the country to refocus on a constructive agenda

What does this mean for my firm?

Firms should familiarize themselves with risk indicators and, where national law requires them to do so, carry out proliferation financing business risk assessments. These should also be built into customer risk assessments. This includes an ongoing review of business risk assessments and customer risk assessments, as well as continuous testing to identify potential sanctions breaches or systems failures that may have led to sanctions breaches.

- **Kosovo and Serbia**: Both countries have been urged to engage constructively in an EU-facilitated dialogue in order to normalize relations

Other global hotspots include:

- **North Korea (DPRK)**: State-sponsored cyber warfare continues to be a major concern and may lead to further sanctions in 2022. It is estimated that the DPRK has a 6,000 member cyberwarfare guidance unit "to conduct financial cybercrime and exploit enemy network vulnerabilities." The US and UN estimated that the DPRK has stolen $3.2bn through cybercrime, including the theft of military information for use in the country's weapons program and extortion through ransomware. The DPRK has also been suspected of involvement in stealing crypto and laundering the proceeds through crypto exchanges. The country has even been found to have attempted a phishing attack on UN sanctions experts. While many of the program's experts are located in Pyongyang, it is thought that parts of the program are operated out of China and parts of Southeast Asia
- **Cuba**: The US imposed sanctions on key officials who targeted peaceful demonstrators
- **Myanmar**: Following the military coup and sentencing of former State Counselor Aung San Suu Kyi for "inciting dissent and breaking covid rules" additional sanctions are possible
- **Ethiopia**: The US has issued sanctions targeting those contributing to the human rights crisis and military conflict in northern Ethiopia, with the EU indicating it is prepared to enact further measures — though it has not yet done so
- **Libya**: Additional sanctions are possible if parliamentary elections in February 2022 are not "free, fair, inclusive and credible" and if foreign fighters are not withdrawn from the country
- **Sudan**: A military takeover in October could lead to sanctions and puts at risk progress made by the transitional government before democratic elections are scheduled in 2023
- **Somalia**: If ongoing elections are not judged to be "peaceful and credible", and humanitarian challenges are not addressed, new sanctions measures are possible
- **Sahel**: The EU has already imposed sanctions on the Wagner Group due to its actions in the Central African Republic. The group is also active in other African countries, including Mali. Sanctions in Chad could be issued due to humanitarian concerns and the need to counter the threat of terrorists in the region

Afghanistan will continue to pose a major challenge as countries determine how to work with the ruling Taliban. Sanctions have been in place against the Taliban for almost two decades, but Afghan-based entities and individuals are also subject to sanctions programs related to counternarcotics, terrorism, Iran, al-Qaida and the Islamic State.

While the worsening humanitarian crisis in the country has been linked to sanctions, the US has issued three general licenses authorizing humanitarian aid. $9.4 billion of Afghan government reserves held in US banks remain frozen.

Going forward, the international community will need to determine how it defines the Taliban now that it leads the country, and if the government should be officially recognized by UN members. The scope of sanctions will also need to be reviewed as the Taliban now controls or oversees the central bank, financial institutions and government ministries.

As a result of actions taken since the Taliban takeover, Afghanistan is increasingly reliant on Pakistan, Iran and China.

OFAC has also issued sanctions against Syria, Lebanon, Libya, Venezuela, Cuba, Iran and terrorist groups including al-Qaida and Hezbollah.

Finally, Brexit opened the way for the UK and EU to develop autonomous sanctions programs, leading to some divergence in sanctions that have been adopted. In April 2021, the UK launched its autonomous Global Anti-Corruption Sanctions program. In November, the EU amended its sanction regime, creating new criteria to allow it to autonomously apply sanctions designations in Mali that go beyond UN measures.

What does this mean for my firm?

Given the quick pace at which the sanctions landscape continues to evolve, firms should ensure that they remain abreast of geopolitical trends and understand how long it takes for their sanctions screening provider to update lists. Firms should also ensure that hotspot countries listed in this section are designated as higher risk, triggering enhanced due diligence and monitoring to more effectively manage sanctions and illicit finance risks. Learn more about the evolving use of sanctions here.

Regional Regulatory Trends and Enforcement

Global

The FATF will continue to have a prominent role in shaping the international AML/CFT regulatory landscape in 2022. The German Presidency, which began in mid-2021 and will end in mid-2022, identified a number of priorities, which the intergovernmental organization will continue to work toward.

These include the incorporation of new technologies to enhance AML/CFT frameworks. To that end, the FATF published two reports in 2021: "Opportunities and Challenges of new Technologies for AML/CFT" and "Stocktake on Data Pooling, Collaborative Analytics and Data Protection." In the former, the task force highlights how financial institutions can utilize new technology when implementing AML/CFT measures. It also stresses the importance of safeguards, such as cybersecurity, data protection and the ability to explain the technology implemented. In the latter, the FATF spotlights the use of big data when identifying patterns yet calls for the adoption of privacy-enhancing technologies.

In addition, rapid user adoption of virtual assets has prompted an increased focus on how criminals can exploit these new asset classes. In June 2021, the FATF published its second 12-month review of the standards and guidelines for VASPs, in which it found there is still significant work to be done. For instance, there is no global framework for "travel rule" compliance — only 15 countries have transposed the recommended travel rule into their AML/CFT regimes — and there are inadequate safeguards to prevent VASPs from being exploited by money launderers.

Due to these findings, the FATF released updated guidance on virtual assets and VASPs in October, clarifying definitions and offering additional recommendations on stablecoins, VASPs and the travel rule. In 2022, this work will continue, with careful attention to mitigating ransomware-related virtual asset risks, ongoing monitoring of peer-to-peer transactions and cross-border payments.

Tackling challenges around gathering beneficial ownership information will also be a priority in 2022 — an issue that was thrown into the international spotlight with the release of the Pandora Papers in October 2021. The FATF issued a public statement on the matter in which it reiterated that it introduced standards on beneficial ownership back in 2003. Yet a review of 100 mutual evaluations revealed that only a third of those countries had laws and regulations that aligned with the FATF's standards. Further, just 10% have implemented measures that effectively ensure transparency of ownership information. The organization also announced it was launching a consultation on improving transparency around beneficial ownership information, and the views collected will inform discussions at the FATF's February 2022 meetings.

The FATF has also made efforts to raise awareness of how the financial system is being used to carry out environmental crimes. The organization has conducted research and met with public and private sector leaders to refine its approach. There's every indication these efforts will continue in 2022.

Other priorities include proliferation and terrorist financing. The FATF issued guidance and reports on both of these in 2021, highlighting the current risks and offering recommendations on identifying and addressing these. It will continue to monitor the evolving terrorist landscape in 2022, updating risk indicators and releasing guidance as necessary.

What does this mean for my business?

Firms should closely follow FATF developments to identify new risk indicators, trends and typologies. That will allow firms to ensure that they are effectively implementing a risk-based approach, are aware of future changes to national laws and regulations, and can prepare accordingly. Customers based in or owned/controlled in countries on FATF gray and blacklists should be subject to enhanced customer due diligence (CDD) and ongoing monitoring.

North America

United States

Modernization has been a key focus for regulators in the US over the past year, and 2022 will be no different.

In June, FinCEN issued the first government-wide list of AML/CFT priorities — a requirement of the Anti-Money Laundering Act of 2020 (AML Act). This list, which includes threats such as corruption, cybercrime, domestic and international terrorist financing, among others, is intended to help financial institutions better marshal their limited compliance resources to combat these challenges. FinCEN is expected to release implementing regulations and additional details shortly.

In addition, 2022 will see steps taken to implement the beneficial ownership amendments in the Corporate Transparency Act, which became law on January 1, 2021. In December 2021, the agency issued a Notice of Proposed Rule Making, which offers more details around who must file reports with FinCEN that provide beneficial ownership information, when to file those reports, and what information is required. There is an opportunity for public review and comment, which closes on February 22, 2022, with implementation expected shortly afterward.

FinCEN launched additional Advanced Notices of Proposed Rule Making on AML/CFT regulations for real estate transactions — including certain non-financed transactions — and antiquities and art. Both would expand reporting requirements and bring more of those involved in these transactions under the purview of the Bank Secrecy Act and other AML/CFT regulations.

Finally, FinCEN issued a Request for Information (RFI) in December, seeking input on ways to modernize the country's AML/CFT approach and identify outdated or redundant provisions that do not align with international standards or a proper risk-based approach. The comment period is open until February 14, 2022.

While many of these efforts may be in the preliminary stages, it is clear that US regulators are poised to make significant changes to the AML/CFT regime. Financial institutions in the US would do well to pay close attention to these developments and devise strategies to implement any changes quickly and efficiently.

Canada

On June 1, 2021, significant changes to Canada's AML/CFT framework, as laid out in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), took effect. The impact of these amendments and the corresponding guidance from FINTRAC is wide-reaching: the areas covered include beneficial ownership due diligence and transparency, virtual currency transaction reporting, new travel rule requirements and obligations for foreign money services businesses and concerning prepaid cards. In addition, there were amendments to the 24-hour rule and updates to customer screening, ongoing monitoring, recordkeeping, employee training, CDD/KYC requirements and PEP onboarding requirements.

Beginning on April 1, 2022, supervisors are expected to initiate compliance assessments that evaluate regulated entities on adherence to the updated AML/CFT framework. FINTRAC has indicated it will show some degree of flexibility when assessing compliance from June 1, 2021, to March 31, 2022. It's worth noting, however, that this flexibility does not extend to certain transactional reporting requirements — although the regulator will allow for a limited ramp-up period from June 1 to December 1.

Additionally, oversight of high-risk sectors, including real estate, casinos, financial entities and money services businesses, will remain a high priority. More specifically, FINTRAC indicated its focus is on client identification and suspicious transaction reporting in real estate transactions. Regarding casinos and money services businesses, the regulator plans to pay more attention to transaction monitoring.

Work will also begin in earnest on creating a comprehensive beneficial ownership registry. As per Canada's annual budget, which was released in April 2021, a total of $2.1 million over two years will go to Innovation, Science and Economic Development Canada to fund the initiative, with completion of a publicly available registry expected by 2025. The long-awaited move will further align Canada with the international standards established by the FATF.

European Union

The AML/CFT landscape in the EU will continue to progress, with major changes expected in 2022.

The most significant change on the horizon is the potential adoption of four legislative proposals that would strengthen AML/CFT regulations within the region.

Central among the proposals is the creation of a new anti-money laundering authority (AMLA) that will oversee AML/CFT efforts across the entire EU bloc. In addition to national regulators, the AMLA will directly supervise certain obliged entities that are high-risk or that handle cross-border transactions. It will also have the ability to impose higher fines. The current expectation is that the AMLA will be established at the beginning of 2023, fully resourced by the end of 2025, and begin direct supervision in early 2026.

When asked which area(s) of AML regulation need to be strengthened, Europe was the only region where "larger fines for AML violations" was the most popular answer, by a margin of eight percentage points. This indicates at least some degree of alignment with the objectives set out for the EU's new AMLA.

A second proposal establishes a new Sixth Anti-Money Laundering Directive (6AMLD) on mechanisms that EU member states must implement or clarify to prevent money laundering and terrorist financing. These include national risk assessment requirements, beneficial ownership register powers and requirements, whistleblower protections and the creation of interconnected, cross-border asset registers that detail bank accounts, safes and real estate, among others.

The third plank of the reform agenda establishes an EU-wide master rulebook, which will not need to be transposed into national law by each member state. Instead, it will be directly imposed across the bloc. The EU also plans to expand its list of obliged entities to include mortgage and consumer credit intermediaries, fund managers offering services to investors in the region, crowdfunding platforms and investment migration operators.

Crypto-asset service providers (CASPs) and virtual asset service providers (VASPs) will also be subject to additional regulations. The proposals would expand the definition of CASPs and increase the scope of obliged entities to align with the Markets in Crypto-Assets Regulation (MiCA). In December 2021, the European Council adopted a negotiating mandate with the European Parliament on a key plank of its planned crypto regulation reform — namely, updating existing rules on accompanying fund transfers to cover crypto-assets.

The fourth and final proposal aims to update regulations regarding funds transfers to bring VASPs into the scope and incorporate travel rule changes.

Firms can explore these four legislative proposals and their implications for compliance teams in our dedicated guide.

EU member states will continue to update their AML/CFT regimes to align with national priorities and comply with EU regulations. Of particular note, however, is Germany. In early 2021, Germany introduced several new measures to strengthen existing AML/CFT laws and transpose the EU's 6AMLD into national law.

Yet this legislation went beyond 6AMLD: instead of establishing predicate offenses, it widens the scope of a money laundering offense to include any proceeds from criminal activity. Then in June 2021, Germany passed the Supply Chain Due Diligence Act, which will enter into force in January 2023. Under this new legislation, companies will need to conduct due diligence and risk analyses on their suppliers to prevent or mitigate international human rights and environmental abuses. As a result, regulators may place more emphasis on going after proceeds linked to human rights abuses, in addition to increased scrutiny on AML/CFT compliance overall.

In January 2022, the European Commission also amended the Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by deleting the Bahamas, Botswana, Ghana, Iraq and Mauritius from the bloc's high-risk country list. The EC determined these countries had taken sufficient steps to address financial crime deficiencies. The Commission noted that FATF public statements, mutual evaluation reports and other international assessments were taken into account. It also added Burkina Faso, the Cayman Islands, Haiti, Jordan, Mali, Morocco, the Philippines, Senegal and South Sudan to its high-risk list.

United Kingdom

The year 2022 will see the UK continue to establish its own AML/CFT regime post-Brexit. HM Treasury, the department responsible for developing and issuing the UK's AML/CFT policies, launched two consultations in July 2021. One focused on the effectiveness of the current regimes and regulations and possible areas for improvement. The other asked for feedback on proposed amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

HM Treasury will publish the outcomes in 2022. But among other changes, the final legislation is expected to include updates to the AML/CFT provisions regulating cryptocurrencies (including the adoption of the travel rule). In addition, the legislation will address asset tracing and recovery, legal barriers to adopting new technology, information sharing and gathering, and proliferation financing. HM Treasury is also likely to publish an updated national Economic Crime Plan — the current plan covers 2019–2022 — which will include a section on anti-corruption.

In September 2021, the UK government published the first National Risk Assessment of Proliferation Financing. As part of its findings, the government concluded that the UK's financial sector has a high risk of being exploited by proliferation actors — and singled out the Democratic People's Republic of Korea and Iran as the most significant threats. It also noted that awareness of proliferation financing risks is lower when compared to other AML/CFT threats. Given these findings, financial institutions can expect that regulators will pay special attention to these risks when assessing compliance programs.

Further, the UK is expected to advance two key pieces of legislation that tackle beneficial ownership. The first is a long-awaited Registration of Entities Bill, which establishes a register of foreign entities that own land in the UK and includes information on the beneficial owners. The initiative was first announced in 2016, and a draft bill was published two years later. There has been little progress since. However, in November, the UK government reconfirmed its commitment to seeing the register through to fruition.

The passage of reforms to the Companies House Registry represents another long-anticipated development. Identity verification for directors and people with significant control of registered companies will be required. In addition, the government will take steps to ensure the accuracy of the information in the register and protect personal information.

Finally, the UK has made an effort to form strategic partnerships to tackle illicit finance and make it easier to do business overseas. In September 2021, the UK announced it had entered into a new partnership with the UAE to combat terrorist financing and organized crime. Then in December 2021, the UK and Singapore signed a Memorandum of Understanding to strengthen the two countries' collaboration on addressing legal and regulatory issues around digital identities.

The UK's rather ambitious agenda in 2022 suggests that the government and regulators are keeping a close eye on AML/CFT threats. Financial institutions and other regulated entities should anticipate more frequent and more severe regulatory action will follow should any compliance gaps be identified.

Asia-Pacific

There are several regulatory developments that financial institutions would do well to keep an eye on in Asia-Pacific this year. Many countries have recently been subject to or will be subject to the FATF mutual evaluation review process. As a result, enhancing AML/CFT laws and regulations will be a top priority, as will the responsible adoption of new technological advancements.

The 2021 survey showed significant regional differences in firms' response to when they chose to incur AML files and violations (Figure 9). 40% of Asia-Pacific firms surveyed said they choose to incur AML fines/violations "all the time," compared to 34% in the Americas and only 30% in Europe. These Asia-Pacific findings were especially pronounced in Australia and Singapore, where 46% and 41% of firms respectively said they choose to incur AML fines all the time.

Philippines

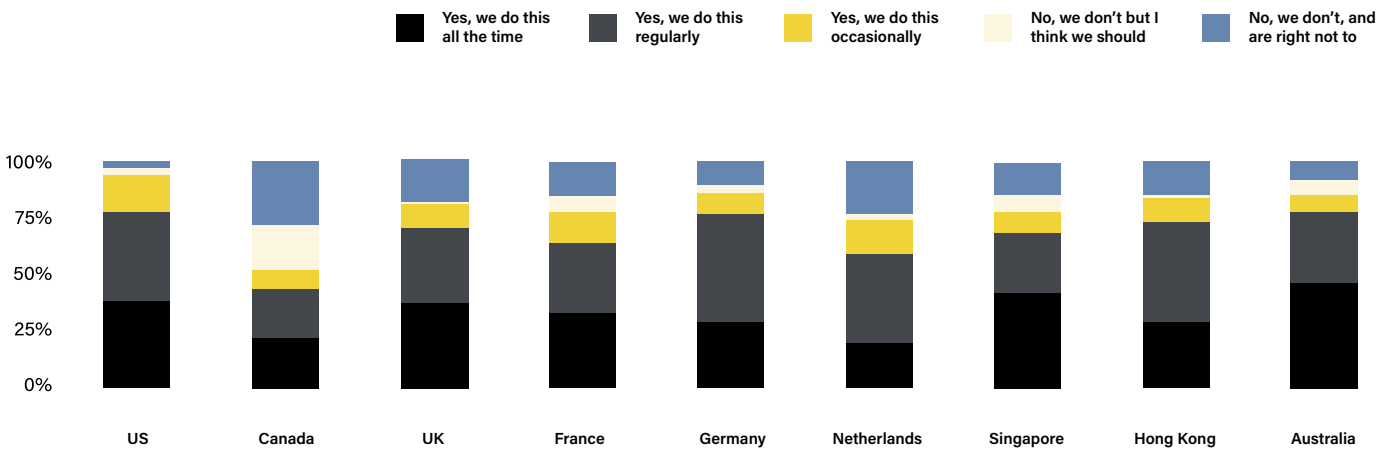
The Philippines has issued a host of new AML legislation, passing the Anti-Terrorism Act of 2020 and amending its Anti-Money Laundering Act (AMLA) in February 2021. The changes brought new entities into scope, including real estate developers, brokers and offshore gaming operators and service providers that are supervised or regulated by Philippine government agencies. New money laundering predicate offenses were introduced, and the country's Anti-Money Laundering Council was given the authority to issue asset freezing orders. Sanctions designation powers were also extended, allowing the Philippines to implement sanctions related to the proliferation of WMDs, terrorism and the financing of terrorism.

Despite these changes, the Philippines found itself on FATF's gray list in June 2021. The country, which must submit progress reports three times a year, was found to lack effective oversight

Does your organization regularly choose to incur anti-money laundering fines and violations with respect to your business decisions and compliance investment? Responses to 'We choose to incur AML fines and make violations'

Figure 9

'ComplyAdvantage: The State of Financial Crime 2022'



of designated non-financial businesses and professions. Other areas identified for improvement include the need to address risks linked to casino junkets, enforce licensing or registration requirements for money or value transfer services, and conduct more financial crime investigations. As a result, regulators will likely be taking a close look at financial institutions operating within the Philippines.

Singapore

The MAS has announced two initiatives aimed at leveraging technology in finance. The first is a centralized digital platform that will facilitate the sharing of customer and transaction information among financial institutions. The MAS is developing the platform with input from six banks, and it is expected to launch in 2023. See the "public-private partnerships" section of this report to explore this in more detail.

In addition, the MAS has announced a new S$42 million grant program, which is designed to "accelerate technology adoption in the financial sector," including the risk management and compliance functions. It also extends the Digital Acceleration Grant (DAG) scheme, which is designed to encourage the adoption of digital solutions to enhance productivity, cybersecurity and operational efficiency. The program is likely to lead to new solutions being developed through 2022.

Other key regulatory announcements from MAS that are likely to help shape the compliance landscape in 2022 include:

- Strengthening AML/CFT Controls of Digital Payment Token Service Providers, setting out MAS' expectations on AML/CFT controls for the digital payment token sector
- Consultation Paper on Proposed New AML/CFT Notice for Precious Stones and Precious Metals Activities and Updates to AML/CFT Notices, exploring the need for specific additional guidance to cover best practices related to precious stones, metals and products processed by financial institutions

2022 may bring additional penalties, with the regulator assessing firms against the new guidance it has issued.

China

Similarly innovation-minded, the Hong Kong Monetary Authority launched a new RegTech Adoption Practice Guide in July 2021 with detailed guidance on adopting RegTech solutions. It also introduced a RegTech Skills framework to foster the development of RegTech talent. Finally, from a general regulatory standpoint, the Securities and Futures Commission in Hong Kong issued updated guidelines on AML/CFT for licensed corporations in September to better align with the FATF's standards.

Even so, Hong Kong's AML/CFT regulatory landscape will be influenced by the actions of Beijing and mainland China, which has introduced its own regulatory updates. In August 2021, new amendments to China's Anti-Money Laundering Law came into effect. The amendments broadened the definition of money laundering, introduced enhanced regulation of non-financial entities, and revised the list of obligated entities to include loan companies, asset management subsidiaries of commercial banks, non-banking payment institutions, insurance agents, and insurance brokers. China has stepped up enforcement of its AML/CFT regulations in recent years, and there has been a notable increase in inspections and prosecutions for compliance failures. This trend is expected to continue in 2022.

In November 2021 China's Personal Information Protection Law (PIPL) came into force. Aimed at establishing a regulatory framework for cybersecurity and data protection in the country, the law has had a significant impact on the maritime sector. The number of Automatic Identification System (AIS) signals in Chinese waters dropped significantly as China blocked public access to shipping location data. China views data derived from AIS signals as a national security threat due to fears foreign intelligence agencies are using it to monitor military vessels. AIS has historically been used as a sanctions tool, with OFAC identifying AIS switch-offs and gaps as a potential indicator of criminal activity.

Companies operating across China must also now employ a data protection officer, with fines for violating personal information rules reaching 50 million yuan, or 5% of a firm's annual revenue. International companies that don't meet their PIPL obligations can also be blacklisted, effectively banning them from processing personal data in China.

Australia

In Australia, reforms intended to strengthen Australia's AML/CFT rules — known as Tranche 1.5 — came into force in June 2021. The changes covered include:

- Changes to CDD, correspondent banking, information sharing and cross-border payment reporting
- Streamlined due diligence requirements for correspondent banking relationships and the prohibition of financial institutions' services being accessed by institutions that allow shell banks to use their accounts
- Guidance on the need for CDD to be completed before a service can be provided
- Clearer rules on third-party reliance, and when SARs can be shared with third parties

Additional reforms, dubbed Tranche 2, are reportedly forthcoming, but there's no firm date or indication that passage will occur in 2022.

AUSTRAC also published guidance to help firms implement AML/CFT reforms, including online regulatory guidance and examples to help firms understand the requirements across customer identification and verification, tipping off, CDD and correspondent banking.

In the 2021 survey, compliance teams indicated they shared many of the same focus areas as regulators. For example, ongoing due diligence of correspondent banking relationships was the area of AML regulation that firms in Asia-Pacific (and the Americas) were most concerned about.

Latin America

In Latin America, countries subject to FATF MERs (Mutual Evaluation Reports), possibly including Argentina, will make changes to their regulatory frameworks to avoid being added to the gray list.

Mexico's government has issued a communique reaffirming that cryptocurrencies are not legal tender in the country and advising of the risks of using virtual assets, including Bitcoin, Ether and XRP. Financial institutions are explicitly banned from offering services to the public that involve virtual assets, including deposits, custody, exchange or transfer.

However, a recent report highlighted that $50,000 million is laundered annually, and Mexico remains one of the world's biggest drug trafficking hotspots. In December 2021, Mexico and the US signed a new Bicentennial Framework, establishing a new security agreement that includes:

- The establishment of working groups on issues including cross-border crimes, the persecution of criminal networks and the reduction of violence
- Priorities such as arms trafficking, a new cybercrimes registry, money laundering and corruption

Africa and the Middle East

The AML/CFT regulatory landscape in Africa and the Middle East in 2022 is expected to undergo a few significant changes, particularly in countries subject to additional scrutiny from the FATF.

The United Arab Emirates has taken a few steps recently to shore up its AML/CFT controls. In 2021, the government established an Executive Office of Anti-Money Laundering and Counter-Terrorism Financing and a special court to try money laundering and tax evasion cases. The central bank also released updated guidance to help financial institutions spot and report suspicious activity. Finally, the country has been working with the UK to strengthen its AML/CFT framework and announced it had officially partnered with the UK to combat terrorist financing and organized crime. Even so, those steps may not be enough to stay off the FATF's gray list. The FATF is expected to take up the matter during its plenary session in February. But regardless of the outcome, the work the UAE has begun will continue throughout 2022.

As of January 2022 several other Middle Eastern and African countries are also currently on the FATF's gray list, including Jordan, Pakistan, Uganda, South Sudan and Zimbabwe. While specific actions have yet to be confirmed, these governments are likely to take steps to strengthen their AML/CFT framework in the coming year.

Kenya is set to undergo its FATF MER in 2022, with huge implications for its Vision 2030 agenda, which sets out the country's roadmap toward becoming an industrializing middle-income country. As part of the plan, the Nairobi International Financial Center was launched to drive investment.

Kenya is also due to issue a national risk assessment soon, flagging AML/CFT threats faced by obliged entities. The MER is likely to lead to legal and regulatory changes in Kenya, including closing loopholes in the legal sector. Greater corporate and beneficial ownership transparency is also possible, with President Kenyatta's overseas assets exposed in the Pandora Papers leak. More guidance for Kenya's banks and thriving FinTech sector is also possible.

What does this mean for my business?

Firms should closely monitor regulatory changes and keep policies, procedures and training materials up to date. They also need to know when and what changes are incoming to identify the right level of resourcing required to ensure that their AML/CFT systems and controls remain relevant and up to date.

Cryptocurrencies and VASPs

Cryptocurrencies and virtual assets went mainstream in 2021 — just 2% of survey respondents said they are not considering crypto services and never will. This means 2022 will see significant developments from a regulatory standpoint. Governments are already taking highly divergent stances and will continue to do so as cryptocurrency and virtual asset adoption increases.

Governments in China and India, for instance, have taken steps to crack down on cryptocurrency trading and mining. No cryptocurrencies, save the country's own digital yuan, are recognized as legal tender in China, and miners have been banned from carrying out activities. In India, the government is expected to introduce a bill that would ban nearly all cryptocurrencies and establish a framework to develop an official digital currency.

At the same time, some smaller countries have embraced digital currencies. In September 2021, El Salvador became the first country to adopt bitcoin as legal tender. Then in December 2021, the National Unity Government, the pro-democracy shadow government that seeks to topple the military regime in Myanmar, announced it would adopt tether as an official currency. This trend of embracing crypto as legal tender, especially among smaller countries or opposition groups, is expected to continue in 2022.

Meanwhile, many other governments are taking a more middle-of-the-road approach to regulation.

The European Commission's adoption of Markets in Crypto-Assets (MiCA), alongside a plan to widen the scope of VASPs and update the travel rule, is an attempt to harmonize regulation and promote market integrity while supporting innovation. Meanwhile, the US is considering proposals to implement a "safe harbor" policy for DeFi and treat stablecoin issuers as banks.

In Asia, the regulation of the crypto market is also gathering momentum. South Korea passed new legislation in March 2021 that required cryptocurrency exchanges and other VASPs to register with the country's financial intelligence unit. The government has also taken steps to require exchanges to partner with traditional banks to ensure the name registered to a crypto account matches the name on their bank account to deposit funds into a virtual wallet. In 2022, South Korea will impose a 20% capital gains tax on virtual asset transactions.

Japan is reportedly considering a strategy similar to that adopted by the US government and may introduce legislation limiting the issuance of stablecoins to banks and wire transfer companies. By contrast, Hong Kong plans to introduce more stringent crypto regulations and limit trading to professional investors with over $1 million in liquid assets.

Divergent regulatory decisions regarding virtual assets aside, there is a clear interest in leveraging the technology that cryptocurrencies and virtual assets are built upon to develop national digital currencies. Several nations and governing institutions — including China, Russia, the UK, the EU and the US — are exploring the development of a central bank-issued digital currency, which promises to bring major changes to the financial landscape.

What does this mean for my business?

Firms operating in the cryptocurrency space should take steps to understand the rapidly changing regulatory landscape and adopt relevant measures. They must ensure that they are not offering services where these are banned and should have the appropriate AML/CFT measures in place to manage risks.

Overview of Enforcement Actions

Regulators are likely to step up their enforcement efforts in 2022. As governments complete their AML/CFT regulatory reviews, modify their sanctions regimes and introduce updated legislation, financial institutions within their jurisdictions will face increased pressure and scrutiny.

As a result, there will be an uptick in fines focused on poor risk assessments, CDD failings, ineffective AML/CFT systems and controls, inadequate ongoing monitoring and reporting of suspicious activity. In addition, as the adoption of digital banking services and virtual currencies becomes more widespread, there are likely to be more fines issued against neobanks, challenger banks, payment transfer companies and crypto businesses.

This is a continuation of the enforcement trends seen in 2021. The US, for example, has maintained its focus on AML/CFT failings but is also looking carefully at these newer asset classes:

- Capital One was fined $390 million in January 2021 for "willful and negligent violations" of AML/CFT laws. Specifically, the bank failed to implement sufficient AML/CFT oversight over one of its business units, the Check Cashing Group, which had many high-risk customers. Capital One also failed to submit currency transaction reports for nearly 50,000 cash transactions totaling over $16 billion

- Robinhood Crypto announced in July 2021 that it expects to pay $30 million to the New York State Department of Financial Services (NYDFS) to settle an investigation into potential cybersecurity and AML/CFT failures

- BitMEX agreed to pay $100 million in August 2021 due to insufficient compliance measures. The cryptocurrency exchange had not implemented an appropriate AML/CFT compliance program and had not filed the required SARs

In the UK, the Financial Conduct Authority has also stepped up its enforcement efforts:

- Credit Suisse was fined £147 million in October for failing to manage its financial crime risk, particularly in its emerging markets business. Despite knowing that Mozambique is a jurisdiction where bribery and corruption risks are high, the bank had facilitated several bribe payments connected to government-sponsored projects in Mozambique

- NatWest was hit with a £265 million fine in December 2021 for inadequate oversight of a high-risk commercial customer, a jeweler. The bank facilitated several large cash payments despite originally deeming the customer too high-risk to permit cash transactions and despite several subsequent red flags. This marks the FCA's first-ever criminal fine for AML/CFT compliance gaps

- HSBC was fined, also in December, £63.9 million. The FCA found that the bank had not maintained effective ongoing transaction monitoring controls. The bank used outdated technology, the parameters to flag transactions were not tailored to the business, and the information fed through the systems was incomplete and inaccurate

In France, the Autorité de contrôle prudentiel et de résolution (ACPR), the national regulator, issued a number of significant enforcement actions through 2021, including:

- Insurer MMA IARD was reprimanded and fined €4 million for failing to detect persons and entities covered by European and national legislation. ACPR found that match rates were too restrictive, with filters of client bases and fund deposits not taking account of spelling variations. MMA IARD had not collected date or month of birth information on more than 42% of its customers, further impacting data quality. Sanctions lists were only updated weekly, instead of daily. As a result of these failings, MMA IARD contracted with an associate that was subject to an asset freeze

- Rakuten Europe Bank was reprimanded and fined €120,000 for a number of failings, including only detecting 90% of PEPs after the start of a business relationship, during weekly screening exercises. As the bank relied on manual processes, there were also periods where no screening was carried out. Other issues included a lack of due diligence on customers, failures in the alert system for transaction monitoring and a failure to report suspicious transactions to TRACFIN, the relevant government agency

- American Express was reprimanded and fined €2 million for its failure to adapt CDD processes to all appropriate risk factors and for the poor collection of identity documents. American Express failed to account for all the risks inherent in its products, the characteristics of customers and geographical factors. For example, some clients were classified as low-risk even though their country of nationality was regarded by the company as high-risk. PEP detection was also inadequate due to incorrect settings in the firm's name screening tool

In Australia, AUSTRAC has issued a number of high profile enforcement actions, alongside a renewed focus on driving cultural change within banks:

- In May, AUSTRAC issued remedial directions to Australian Military Bank, requiring it to conduct an ML/TF risk assessment of its business and provide regular reports on its progress

- In June, National Australia Bank (NAB) was informed that AUSTRAC had identified serious concerns with its AML/CFT compliance in relation to customer identification and due diligence. A formal enforcement investigation is underway

- In November, Westpac agreed to pay penalties totaling $113 million, with the bank criticized for its "poor compliance conduct." In September 2020, the bank paid a record $1.3 billion fine for non-compliance with money laundering and child exploitation regulations

- In January 2022, AUSTRAC announced it was expanding the scope of its investigation into the Star Entertainment Group as a result of potential non-compliance with AML/CFT rules in its casinos

In January AUSTRAC also issued a statement praising banks in the country for improving their compliance programs, enabling the regulator to focus on other areas of financial crime risk, including crypto exchanges, casinos, pubs and clubs.

Other notable fines include:

- In January, the Central Bank of the United Arab Emirates hit 11 banks with fines totaling $12.4 million. That marked the regulator's first enforcement action since 2020 when the FATF published a scathing critique of the country's AML/CFT controls

- AmBank confirmed in February that it would pay the Malaysia Central Bank $700 million to settle claims linked to the 1MDB scandal

- ING Bank was fined €3 million in March by the French regulator, the ACPR

- In April, ABN Amro announced it had settled with Dutch authorities and would pay $574 million

- The following month, Nasdaq Stockholm's disciplinary committee determined Swedbank would pay a $5.5 million fine, and the Financial Supervisory Authority of Norway fined DNB Bank $4.81 million

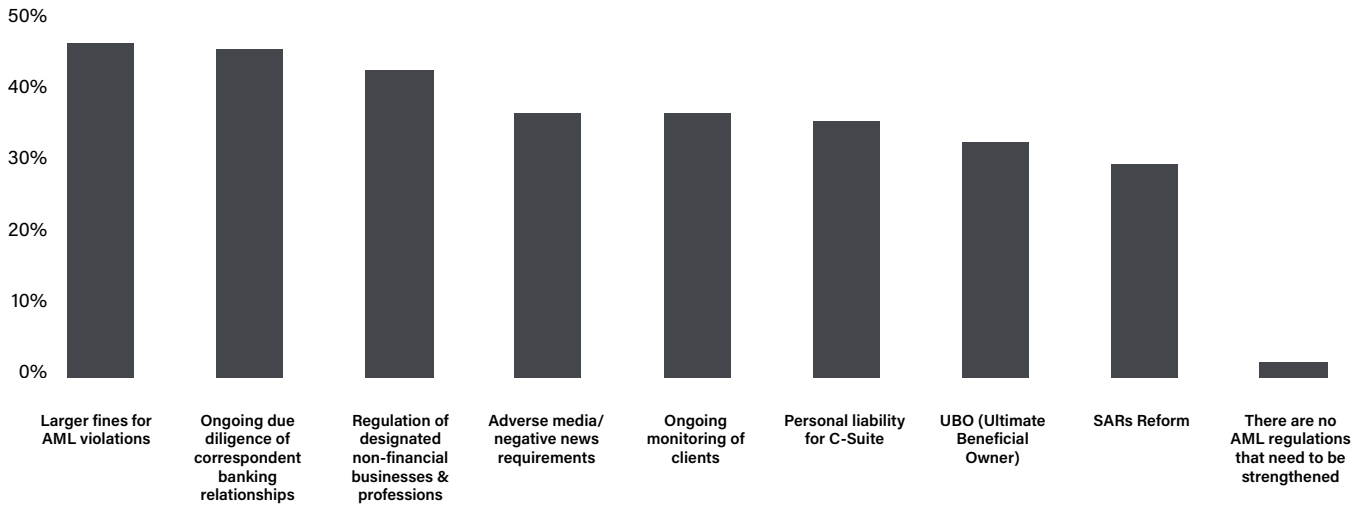
In all these enforcement actions, regulators cited AML/CFT shortcomings as the primary issue. This sampling of fines underscores the need for an effective compliance program — one that is comprehensive and includes transaction monitoring, regular risk-based assessments and appropriate monitoring of foreign subsidiaries, intermediaries and correspondent banking relationships.

Globally, with respect to anti-money laundering fines, there were notable increases in the number of firms saying they consider the risk of incurring a fine or violation (from 38% in 2020 to 52% in 2021) and in firms saying they choose to incur AML fines and make violations "all the time" (from 25% up to 35%). More than a third of firms surveyed globally now say they choose to incur AML fines and violations all the time.

Despite this, only 2% of those surveyed felt no areas of AML regulation in their country needed to be strengthened (Figure 10). The main areas where organizations said there was room for improvement were: larger fines for violations (47%), ongoing due diligence of correspondent banking relationships (46%) and regulation of Designated Non-Financial Business and Professions (DNFBPs) (43%).

Which area(s) of AML regulations need to be strengthened in your country? *Figure 10*

'ComplyAdvantage: The State of Financial Crime 2022'



What does this mean for my business?

Firms should review enforcement actions issued by their local regulators to identify areas of focus for regulators. Firms should also carry out assurance testing and confirm their AML/CFT systems and controls are up to date. Finally, if they are subject to intrusive regulatory supervision, they must ensure that they are open and honest with the regulator.

Industry Trends

When asked what factor was most likely to drive change in their organizations (Figure 11), firms cited regulatory enforcement action (39%), followed by a competitor threat (33%). There was, however, some divergence in this trend at the country level. Regulatory enforcement was the biggest factor by a considerable margin in Australia (45%) and Singapore (45%). In Canada (40%) and France (38%), a competitor threat was the factor most likely to drive change — again by a considerable margin.

Which of the following events is most likely to drive change within your organization?

'ComplyAdvantage: The State of Financial Crime 2022'

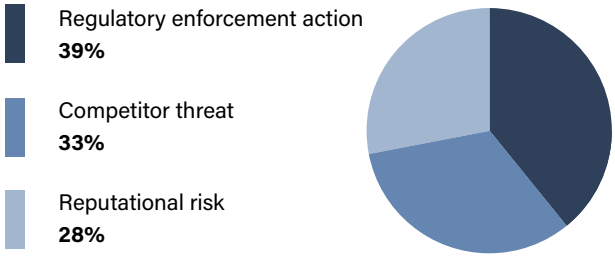


Figure 11

These conflicting results speak to the tension many firms feel between the need to innovate continuously, onboard customers quickly and offer services in near real time while avoiding the consequences of regulatory enforcement action.

With remote/hybrid working now the norm, and firms grappling with ever-growing volumes of data, upgrading legacy technology remains a top priority in 2022.

Investment in RegTech Continues

With these challenges in mind, compliance teams said the main areas in their departments they are looking to improve in 2022 are upgrading legacy technology systems (27%), managing and using data (26%) and how they work with third party suppliers (19%).

When asked specifically where they will prioritize current and future investment in AML solutions, organizations pointed to dynamic risk scoring of customers and dynamic risk scoring of transactions (both 47%), followed by transaction monitoring (45%).

At the core of many of these focus areas are AI and data analytics and the potential these innovations can offer to combine datasets and enable more real-time risk assessments. A keynote speech by the assistant managing director of the MAS in August 2021 explored how firms can deliver on this potential, breaking down the deployment of data analytics into three levels:

- **Customer**: Using the latest technologies, firms can now shift from cycle-based periodic risk assessments to a more dynamic approach. However, MAS highlighted that "there needs to be sufficient validation of increased effectiveness over existing practices and also involves upskilling of staff to recognise, prioritize and act on the risk signals"

- **Network**: Simply focusing on customers and entities risks missing the bigger picture. Network analysis is key for uncovering shell/front companies and beneficial owners in sectors such as wealth management. MAS noted that it "similarly leverages STR [Suspicious Transaction Reports], intelligence and other data points to perform network link analysis to detect emerging threats or suspicious activities"

- **System**: MAS also highlighted the need for better collaboration between institutions, stating that technological advances here could "bring us closer to a turning-point

The FATF reports on technologies and data mentioned earlier are also an invaluable guide as firms look to upgrade legacy systems. The FATF highlights the importance of new solutions being explainable. It also mentions examples of how new technologies can support AML/CFT effectiveness, including digital identity, national language processing, application programming interfaces (APIs) and distributed ledger technology (DLT). The FATF's report on data pooling, analytics and protection also recognizes the ability of firms to more efficiently identify trends and patterns using big data and calls for the adoption of privacy-enhancing technologies.

Any firm that is upgrading legacy systems or introducing new solutions into their AML/CFT operations should review these documents as part of their internal evaluation processes. Compliance and financial crime prevention officers should also be aware of and understand the types of technologies that are available for AML/CFT and how they could be used to enhance their own programs. You can find out more about maximizing the effectiveness and efficiency of customer screening here.

Enhancing the detection of PEPs and RCAs

As was noted earlier in this report, the issue of PEP and RCA detection was thrown back into the spotlight by the Pandora Papers, with 48% of compliance teams globally saying the detection of these groups is the area of their AML program they're most focused on improving. These findings reflect the growing challenges of PEP detection: a global financial system underpinned by a plethora of regulations at the state level, alongside the use of complex legal mechanisms by some PEPs and RCAs to conceal illicit behavior.

This is an area where compliance teams are in alignment with the FATF. In November 2021, the FATF published proposals for amending Recommendation 24, which is designed to increase transparency around the beneficial ownership of legal persons. The FATF plans to introduce stronger language on the misuse of legal persons for money laundering, the prohibition of bearer shares and a requirement for countries to establish a beneficial ownership registry.

Weeks later FinCEN issued a notice setting out new rules on who must report beneficial ownership information, when they must report it, and what information they must provide. The EU's draft AML/CFT Regulation (AMLR), published in 2021, also lays out more detailed requirements on ultimate beneficial ownership, including how to determine who should be subject to enhanced ID checks and how to determine control for beneficial ownership transparency. Directors and shareholders must be registered in the EU, and non-EU entities must register UBOs when entering into a business relationship in the EU or acquiring real estate. The EU's new planned AMLA will also allocate a risk rating to obliged entities — with one qualitative part of the assessment being the share of PEPs an entity has as a proportion of its overall customer population.

Improvement in PEP and RCA detection processes more widely have been driven by FATF MERs. In the Philippines, the Securities and Exchange Commission introduced measures to boost transparency in corporate ownership structures. Firms that do not comply face financial penalties. Hong Kong's FIU also announced it would amend the definition of PEPs to include individuals outside of its territory. This came in response to Hong Kong's 2019 MER, which stated that a failure to cover PEPs from other parts of China in the region's AML program was a "technical gap."

The survey noted two areas that are likely to become a focus of efforts to enhance the detection of PEPs in 2022: global coverage and RCA detection. Comprehensive coverage of both of these areas is key to a truly risk-based compliance program, as well as fully assessing and understanding beneficial ownership structures. When asked what areas of PEP screening solutions their firm most values (Figure 12), 39% said global coverage, and 31% said relatives and close associates. Find out more about how dynamic global coverage can enhance PEP screening.

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

'ComplyAdvantage: The State of Financial Crime 2022'

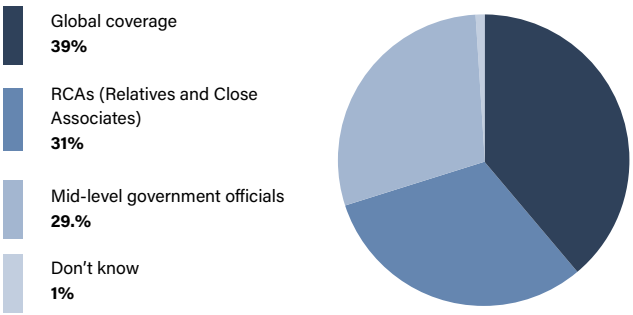


Figure 12

Public-private partnerships expand with innovative technology

Regulators in the Asia-Pacific region are continuing to lead the way in developing innovative public-private partnership arrangements — a trend that is likely to continue, and expand globally, in 2022. While such partnerships have existed in many countries for some time, new solutions built on innovative technology platforms are enabling deeper and more sophisticated collaborations between regulators and financial institutions.

The MAS has been a leading innovator in this space, announcing in October 2021 a groundbreaking digital platform to facilitate information sharing between major banks. Due to be introduced in 2023, the Collaborative Sharing of ML/TF Information and Cases (COSMIC) will enable financial institutions in the country to digitally warn each other about unusual activity in customers' accounts. The platform was co-created by MAS and six commercial banks — DBS Group, Oversea-Chinese Banking Corporation, United Overseas Bank, Standard Chartered Bank, Citibank and HSBC. COSMIC will initially launch with the involvement of larger banks, but MAS plans to roll the program out progressively to more financial institutions and focus areas — a trend other regulators could follow.

The Fintel Alliance, established by Australia's regulator, AUSTRAC, is another public-private partnership that has continued to develop its approach. In its 2021 Fintel review, AUSTRAC highlighted that 5,258 SARs were lodged relating to the focus areas for Fintel. Its 2020-2023 operational strategy also focuses on improved approaches to information sharing through a supporting technology-based infrastructure. AUSTRAC notes that this platform has been key to continuing information sharing through the pandemic. Going forward, the focus will be on enabling higher classification information to be shared.

In 2022, the European Commission is looking to use its supra-national role to facilitate more effective public-private partnerships across the European Union. This follows a consultation in 2021 designed to understand what public-private partnerships currently exist, which private sector entities participate and how the success of such partnerships could be measured in the future.

2022 also sees the UK's current Economic Crime Plan come to an end. Among its core goals is the development of stronger public-private partnerships. The UK government is particularly focused on "the need to engage smaller and geographically-diverse organizations to ensure the full range of economic crime is being addressed." The plan further emphasizes the importance of engagement with sectors not covered by anti-money laundering regulations including social media, telecommunications and technology companies.

Banking the Most Sought After Hiring Background

Firms are having to work harder than ever to attract top talent from their preferred industries. The top background compliance teams want to hire from in 2022 is banking (Figure 13), which was selected by 27% of respondents. This was followed by FinTech (19%), crypto (18%) and law (17%).

The only sector where this differed was crypto exchanges. 68% listed other crypto firms as their preferred hiring background, followed by fintechs and regulators.

With respect to hiring for your organization's compliance team, which industry background do you most recruit from?

'ComplyAdvantage: The State of Financial Crime 2022'

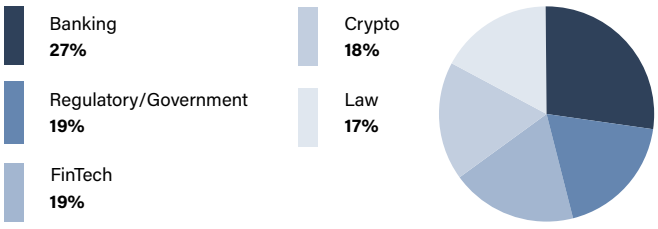


Figure 13

When selecting new hires, firms need to balance:

- **Generalists vs. specialists**: Some organizations, especially those experiencing rapid growth and/or at an early stage are often tempted to focus on compliance hires who can cover multiple functions. However, many find themselves re-evaluating their searches to focus on specialists who can cover priority functions (e.g., fraud) in more detail

- **Type of experience**: Compliance staff from larger firms will most likely have had access to training and support not available to those operating in smaller and start-up environments. This can make them attractive hires — especially if they come with up-to-date qualifications a firm would otherwise have to invest in. However, other hiring managers will prefer candidates who have experience in a more "hands-on" environment, managing rapid growth and roving across a wider portfolio of activities. There's no right or wrong background, so organizations need to consider the pros/cons of different types of experience

- **Cultural fit**: While compliance teams should be aligned around their organization's wider vision, for some firms — especially highly mission-driven firms such as FinTechs and digital banks — there is a risk of "self-confirmatory bias," where all employees come from similar backgrounds. Hiring managers need to balance the importance of a coherent team with the need to bring in perspectives that will challenge existing assumptions

Adoption of Crypto Accelerates

While it's clear 2021 was the year when crypto went mainstream, in terms of maturity, the market is far from homogeneous. 49% of firms said they accept or work with crypto, 22% are crypto-native, and a further 21% are evaluating offering crypto.

This is reflected in — and driven by — shifts in consumer behavior. In August, blockchain data firm Chainalysis published its second-ever global cryptocurrency adoption index, which reported an 880% rise in global crypto adoption, driven by peer-to-peer (P2P) trading and usage in emerging markets such as Africa. The Chainalysis team tracked data across 7,000 crypto service providers and found "meaningful crypto activity" in 158 countries.

The FATF's guidance for a risk-based approach to virtual assets, referenced earlier in relation to regulatory compliance, can also be informative when assessing the acceleration of the crypto industry. It provides an important look at how virtual assets and VASPs are defined, how the FATF standards apply to stablecoins, guidance on licensing and an update to the implementation of the travel rule.

Firms looking to launch, develop and refine their crypto and virtual asset-based products should review the latest FATF guidance alongside updates from national regulators to ensure they're fully compliant. Where possible, proactively updating regulators on product roadmaps is also critical.

Timelines

February

14 – 18 Feb – GIABA Plenary

14 – 22 Feb – FinCEN Bank Secrecy Act consultation closes

27 Feb – 4 March FATF Plenary; possible discussion of FATF Mutual Evaluation Reviews (MERs) of the following countries: France and Indonesia

April

1 April – Canada to begin compliance assessments against PCMLTFA

Possible discussion of FATF Mutual Evaluation Reviews (MERs) of the following countries: Namibia (ESAAMLG) and Liechtenstein and Bulgaria (MONEYVAL)

June

12 – 17 June – FATF Plenary; possible discussion of FATF Mutual Evaluation Reviews (MERs) of the following countries: Germany and the Netherlands

UK Treasury to publish a report on the review of the MLRs and OPBAS regulations

Updates to UK's High Risk Third Country List

March

Possible discussion of FATF Mutual Evaluation Reviews (MERs) of the following countries: Equatorial Guinea and Congo at GABAC

Updates to UK's High Risk Third Country List

10 March – Deadline to register on UK's Trust Registration Service (TRS)

May

Possible discussion of FATF Mutual Evaluation Reviews (MERs) of the following countries: Aruba, Grenada, St. Vincent and the Grenadines, Dominica and Venezuela (CFATF) and Cote D'Ivoire and Gambia (GIABA) and Gabon (GABAC)

July

1 July – New FATF President Appointed

Possible discussion of FATF Mutual Evaluation Reviews (MERs) of the following countries: Ecuador (GAFILAT) and Nauru, Niue, Papua New Guinea, Timor Leste and Afghanistan (APG)

August

Possible discussion of FATF Mutual Evaluation Reviews (MERs) of the following countries: Curacao (CFATF)

October

16 – 21 Oct – FATF Plenary

Updates to UK's High Risk Third Country List

December

Finish establishing AMLA in Europe

September

Possible discussion of FATF Mutual Evaluation Reviews (MERs) of the following countries: Kenya (ESAAMLG) and Chad (GABAC)

November

Possible discussion of FATF Mutual Evaluation Reviews (MERs) of the following countries: Liberia (GIABA), Anguilla (CFATF), Guinea (GIABA), Bolivia (GAFILAT), Kazakhstan (EAG)

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 800 enterprises in 69 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 Goldman Sachs Growth Equity Fund, Ontario Teachers', Index Ventures and Balderton Capital. Learn more at:

Our Customers

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

Get in Touch

AMER

New York

1460 Broadway
#8000
New York
NY 100136

P +1 (646) 844 0841
contact.usa@complyadvantage.com

EMEA

London

LABS House
15-19 Bloomsbury Way
Holborn
London WC1A 2TH
United Kingdom

P +44 20 7834 0252
contact.uk@complyadvantage.com

APAC

Singapore

26 China Street
#02-01 Far East Square West Plaza
Singapore
049568

P +65 6304 3069
contact.sg@complyadvantage.com

EMEA

Romania

34-36 Somesului street
Cluj-Napoca
Romania
400145
P +40 752 647 872

For details on the source materials used in this guide, please visit complyadvantage.com/insights