The State of Financial Crime 2021

Technology, regulation, and the future of financial crime compliance

ComplyAdvantage

Contents

01

Executive Summary

COVID-19 & Digitization

The shift to a digital world is creating many opportunities, like authorized push payment fraud, that can be exploited by criminals.

Takeaway
Firms should update their risk enterprise-wide assessments to take account of digitization trends and identify ways to keep employees connected and motivated.

Spotlight on Financial Crime

Financial crime developments will range from addressing insights revealed by the leak of the 'FinCEN files' in the US, to the convergence of fraud, cyber, and money laundering, the rise of crypto, and the ever-changing sanctions landscape.

Takeaway
Firms will need to ensure that they have robust, flexible, and integrated screening and monitoring systems in place to navigate the complexities of different types of financial crimes.

Trends in geopolitics & Impact on Financial Crime

Geopolitical events in the world can disrupt businesses and reshape illicit finance operations, creating new criminal ventures and regulatory requirements that firms must identify and manage as part of their AML/CFT programs.

Takeaway
Firms should follow global trends as part of their horizon scanning activities and be prepared to quickly update AML/CFT policies, processes, and procedures to ensure that they remain on the right side of the law.

Regulatory Change and Enforcement

A plethora of regulatory changes will take place as governments seek to respond to new financial technologies, such as Virtual Assets, and promote the use of technology to tackle financial crime which raises regulatory expectations and leads to stronger enforcement.

Takeaway
In addition to incorporating regulatory changes into AML/CFT programs, firms will need to ensure that they support their assurance and audit functions in identifying and addressing potential regulatory issues.

Industry Trends

RegTech adoption, COVID-19 linked crime, the rise of crypto, and the creation of innovative solutions through public-private sector collaboration are some of the trends to be on the lookout for.

Takeaway
Firms should be ready to address new threats, engage in cross-industry dialogue and seize opportunities to innovate as industry trends change quickly.

02

Introduction

Welcome to ComplyAdvantage's outlook for 2021, a year that will continue to contend with the fallout of the Covid-19 pandemic and anti-money laundering data leaks.

Compliance has always been challenging. Compliance officers have to educate organizations on emerging threats, the implications of evolving regulations, and the onslaught of criminal behavior while balancing their organizations' risk appetite. Meanwhile, the monitoring and reporting of suspicious activity place organizations on the frontline of managing financial crime risks on behalf of governments.

Last year proved to be a difficult year as Covid-19 changed the way organizations worked. That, compounded by regulatory divergence, the escalating use of sanctions, and an increase in cybercrime and fraud activity, forced organizations and governments to think critically about their anti-financial crime efforts. In the final months of 2020, ComplyAdvantage interviewed 600 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 dive deep into the challenges organizations face and give us a glimpse at the trends that are likely to emerge in 2021. A look at the numbers:

- SARs filing was on the rise with 74% of respondents saying they filed more SARs in 2020 than the previous year
- While several countries are in the process of introducing critical updates to their AML regulations, only 19% of respondents felt that AML regulations needed to be strengthened
- 93% of respondents stated that real-time AML risk data would improve their compliance operations
- Improving fraud detection ranked highest with 69% of respondents indicating fraud as a significant driver of financial crime in 2020

In 2021, firms will face many challenges. Fraud, cyber, and money laundering will continue to converge as criminals exploit grand-scale digital adoption through computer and mobile-enabled crime. Geopolitics, particularly the 2020 US election, Brexit, the destabilizing effects of Russia, the rise of China, and political unrest, will change how criminal networks operate and how countries use AML/CFT tools to retaliate. Corruption will continue to become more attractive as trillions of dollars channel through the international system via economic stimulus measures, but also to support the delivery of vaccines.

Against this backdrop, lawmakers, particularly in the US and European Union, have pledged to make the AML/CFT frameworks more effective and have begun implementing the many legal and regulatory changes to do so. Hong Kong, Singapore, and the UK will further promote technological adoption and innovation. Brexit will affect how the EU and the UK work together, and the UK will expand its autonomous sanctions regime. The Financial Action Task Force (FATF) will continue to set the global AML/CFT agenda under the German Presidency, with the current President, Dr. Marcus Pleyer, likely to encourage a more granular exploration of the use of RegTech for AML/CFT purposes. FATF will also continue its country assessments in the 'Fourth Round' of mutual evaluations, driving further enhancements in national frameworks as countries such as Pakistan seek to avoid the economic and political consequences of remaining on the organization's 'grey list' of countries with significant AML vulnerabilities.

Firms will need to embrace the risk-based approach to manage finite resources against an onslaught of criminal activity; and as the Covid-19 pandemic unravels, firms will need to be more creative in monitoring, training, and motivating employees working from home.

2021 will be a year of opportunity to innovate and learn how to use data and technology to support efforts to fight financial crime.

03

COVID-19 & Digitization

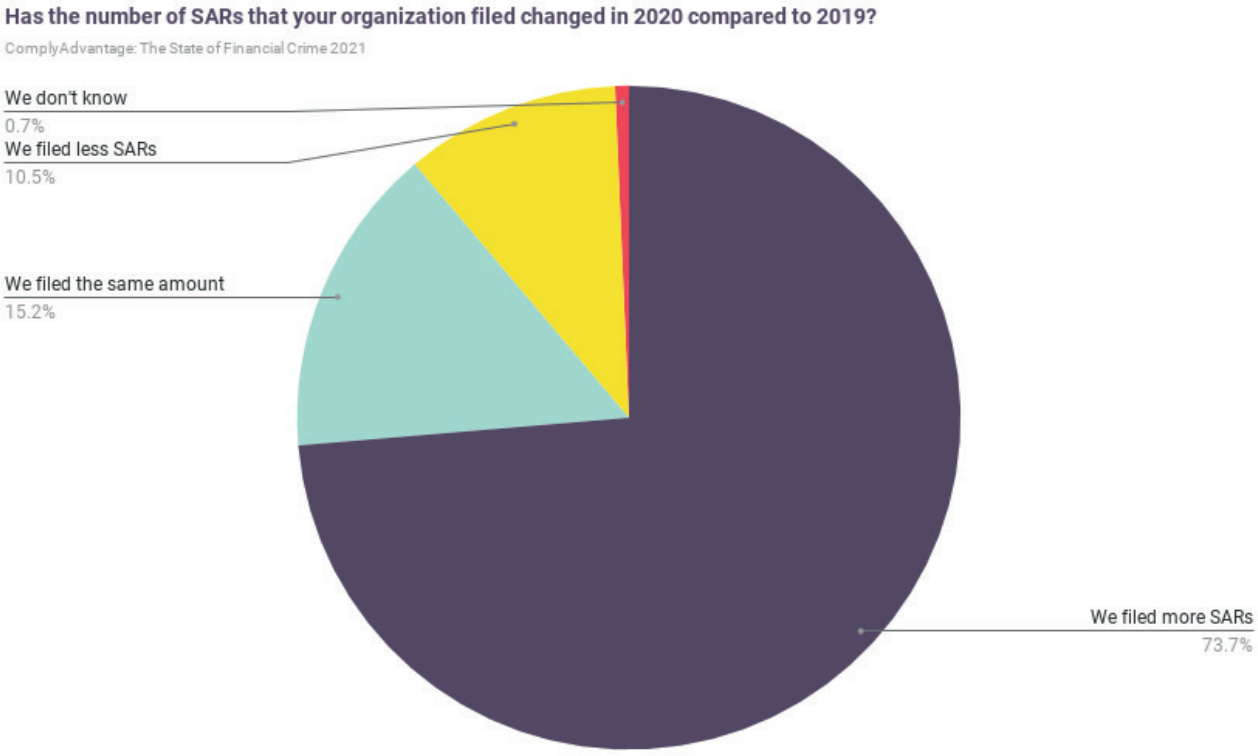
Financial institutions reported that the top three things Covid-19 put pressure on were: increased fraud cases, risk appetite, and operational processes. This is likely to continue into 2021 as the world continues to cope with the pandemic and embrace technological adoption. In 2020, G20 countries committed to spending US$21 billion, injecting US$11 trillion into the global economy, and releasing US$14 billion in liquidity to allow indebted countries to fight the pandemic. The astronomical amounts of public funds flowing through the international financial system have created a honey pot for criminals and corrupt actors. Governments will continue to walk the fine line between making funds and support available to vulnerable individuals, companies, and countries at pace while putting in place measures to tackle fraud and financial crime in a frictionless manner.

Economic stimulus measures, aid funding, investments into health infrastructure, and the development and distribution of Covid-19 vaccines were vulnerable in 2020 and will remain vulnerable to criminals in 2021. Interpol has warned that as Covid-19 vaccines are approved and released, organized crime groups (OCGs) will try to steal vaccines, selling them at profit or simply selling fake variations. The Financial Action Task Force (FATF) warned of numerous Covid-19-related risks including fraud, cybercrime, exploitation of economic stimulus measures, and Virtual Assets Service Providers (VASPs) laundering the proceeds of the sale of Covid-19 vaccines.

The shift to remote working and national lockdowns has led to the quick adoption of e-commerce and digital and instant payments, leading to cash displacement in many jurisdictions and disrupting criminal payment corridors. Before the pandemic, digital payments growth was estimated at 12.7% and expected to produce 726 billion transactions annually in 2020, with an estimated 60% of world GDP digitized by 2022. This now appears to be an underestimate. Tokenized payments and crypto assets will increase and more Central Banks will pilot the use of digital currencies. All of these changes will speed up the adoption of non-face-to-face automated customer onboarding and digital ID.

These changes will also have a major impact on firms' ability to monitor transactions. Legacy monitoring systems, often based on relatively inflexible rules, will continue to struggle to cope with the fast-changing customer and criminal behavior as governments test different responses to the pandemic and global economic depression. While there were many factors at play, it is not surprising that 74% of respondents said they filed more SARs in 2020 than in 2019. 2021 will likely surpass 2020 as new types of technologies and different ways of monitoring transactions will need to be explored to allow firms to contend with the exponential increases in volumes as well as the new and varying payment channels used by one single customer via different devices, including mobile money, SWIFT, instant payments, crypto, and distributed ledger technology all while working remotely. This will likely stimulate and drive forward RegTech adoption, and the risk-based approach will become key in helping firms decide where to allocate their precious resources.

As criminals exploit home working arrangements, firms will continue to face challenges in managing financial crime risks while their employees work remotely. Malicious actors will continue targeting employees and businesses to gain access to sensitive data or systems. And of course, there is the need to keep people motivated and upskilled to face new threats and challenges, requiring dynamic virtual training and constant reminders to report suspicious activity while managing compliance fatigue. From a systems perspective, more data and processes will be transferred onto the cloud and new vendors will be onboarded to cope with rising transactional volumes and drastic changes in customer behaviors. Updates to policies and procedures will continue to be carried out remotely, requiring firms to explore ways of capturing the attention of world-weary staff.



What does this mean for my business?

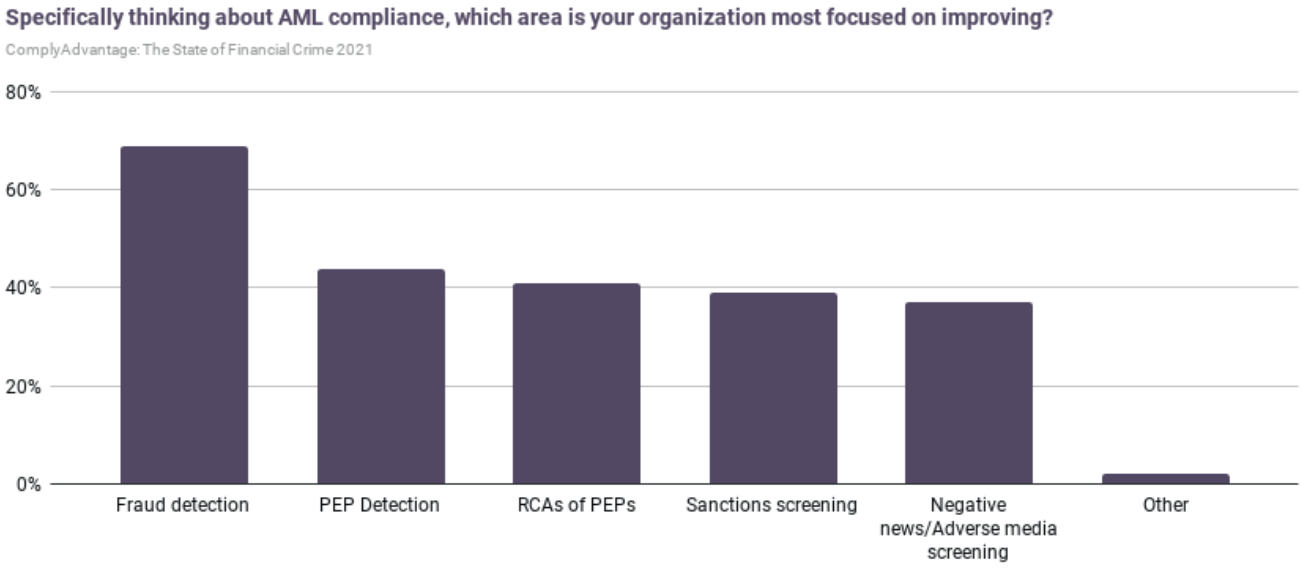
Firms should look to ensure that enterprise-wide risk assessments capture new threats and risks created by Covid-19, but also posed by employees operating in remote locations and virtual environments. As new technology is onboarded and new payment methods and channels are introduced, firms should document associated AML/CFT risks; and how they are managing them to ensure that they do not expose their firms and customers to enhanced financial crime threats. Firms will also need to work closely with RegTech providers to understand their abilities to scale, manage workflow, and report management information to allow them to manage their own risks. Finally, firms will need to manage insider risks and adopt new ways of motivating and monitoring employees working from home, potentially on their own devices without security controls that would be in place in a normal working environment.

04

Spotlight on Financial Crime

The world of financial crime is far-reaching. With cybercrime and fraud on the rise, criminals are continuing to prove resilient and innovative. Compliance officers are tasked with balancing new regulations, increased use of sanctions, and the evolution of financial crime. When asked what predicate offenses are most important for their organization, fraud took the top slot. It is not surprising then that organizations around the world are focused on improving fraud detection. Politically Exposed Persons (PEPs) and Relatives and Close Associates (RCAs) detection quickly followed. With economic stimulus measures, crisis-related humanitarian funds, and disinformation around Covid-19 financial institutions face increased pressure to uncover hidden risks and corruption.

The following section will shine a spotlight on Financial Crime, exploring how the financial crime and regulatory landscape will be shaped by last year's leak of US SAR data, known as the 'FinCEN files'; the convergence between fraud, cybercrime, and money laundering; sanctions trends; cryptocurrencies and Virtual Assets Service Providers; and evolving fundraising methods for terrorist financing.



FinCEN Files

The release of the FinCEN Files shed light on the inconsistencies in the global anti-money laundering (AML) and counter financing of terrorism (CFT) system. The 2,500 leaked Suspicious Activity Reports (SARs), held by the US Financial Intelligence Unit FinCEN, showed that between 1999 and 2017, top tier banks reported over $2 trillion worth of transactions with clients in over 170 countries. These clients included organized crime groups, oligarchs, and corrupt businesses tied to PEPs. Investigations connected funds transfers to arms dealers and ivory, gold, and diamond traders in Africa; sanctions evasions and doping and bribery schemes in the Middle East; and football corruption and the exploitation of food and housing programs for the poor in Latin America. The leaks highlighted the use of several major northern European banks as laundromats for malicious actors, especially from the countries of the former Soviet Union, and underscored the abuse of corporate structures and the investment versus the effectiveness of financial crime prevention efforts.

The FinCEN Files shined a harsh light on the fractures of the SARs regime, shattering the notion that SARs are protected disclosures. For example, in the United States financial institutions have 30 days to file a SAR, or 60 days if more time is needed to identify the entity, but the report highlighted that the median time was 166 days. The leaked SARs also emphasized law enforcement's insufficient resourcing, dated technology systems, and non-existent feedback loops that negatively affect their ability to take action on SARs. While the FinCEN Files will impact active investigations for years to come, the leaks proved further impetus for legal and regulatory reform in countries like the US and the United Kingdom (UK).

In the UK, the FinCEN Files identified over 3,000 UK-registered Limited Liability Partnerships (LLPs) and Limited Partnerships (LPs), half of which were incorporated by the same agencies linked to the Baltics. More than 1,000 companies had the same address, and many shared the same mailbox address, signatures, and nominee shareholders. To tackle these deficiencies, the UK government will give the UK corporate registry, Companies House, the powers to remove false information and mandate that only Trust and Company Service providers can incorporate entities. Verification of identity checks for all directors, controllers, and those filing information on behalf of the company will also be introduced and Companies House will require evidence of checks. The attention brought to corporate transparency should also accelerate the development of the Register of Overseas Entities Bill to identify foreign owners of property in the UK in 2021. Successful implementation of these changes will need the institutions involved to have the resources necessary to make them effective, however, and Companies House is already under-resourced at present.

In the US, FinCEN will move forward with implementing changes following its consultation on proposals for making AML programs better at fighting financial crime. The leaks revealed that several top banks previously fined for AML/CFT failures continued to move funds for suspicious actors, raising questions about how effective AML/CFT can be when it mandates that financial institutions only report suspicious activity, rather than interdict it. Proposed changes include publishing a regulatory definition of what constitutes "AML program effectiveness" and issuing guidance to provide further clarity around actions necessary to comply.

In response to the FinCEN consultation, a number of banks indicated that they welcomed guidance on effectiveness but would like to see clearly communicated priorities and further regulatory support. This led the US government to move forward with the National Defense Authorization Act (NDAA) 2021. The NDAA includes numerous changes to make the fight against AML/CFT more effective. This includes calling on businesses to carry out business-wide risk assessments, test, and monitor record-keeping and suspicious reporting requirements on an on-going basis, and provide "useful information" when filing SARs. The NDAA also introduces provisions on strengthening financial intelligence and AML/CFT programs, modernizing the AML/CFT system — with a particular focus on the use of technology and data sharing, enhanced AML/CFT communication, oversight and processes, and will create a national beneficial ownership registry at FinCEN.

What does this mean for my business?

Firms will need to ensure that they monitor US and UK regulations to identify new changes. When changes come out, firms should carry out gap analysis and identify actions that will allow them to meet the definition of "effectiveness." Firms should also understand different types of criminal activity that are prevalent in the jurisdictions in which they operate to arm staff with the appropriate tools to respond and manage risks.

Convergence between Fraud, Cybercrime & Money Laundering

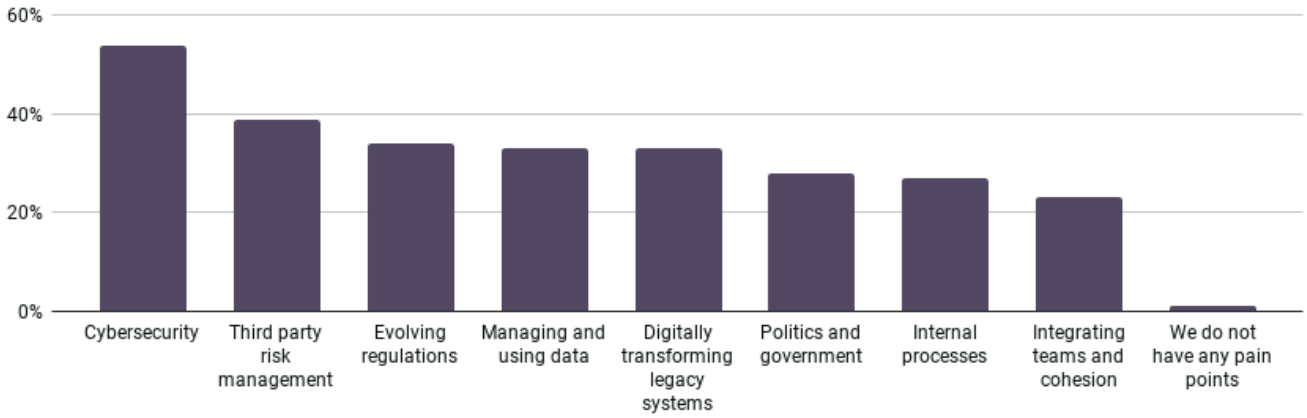
Computer and mobile-enabled fraud proliferated in 2020. Cybersecurity and third party risk management were noted as organizations' biggest compliance-related pain points in 2020. With 54% of respondents ranking cybersecurity as a top pain point. By the end of 2020, Singapore had indicated that cybercrime cases had risen by more than 50%. This followed a trend; ransomware attacks had increased by 50% in daily average attacks, with the US, India, Sri Lanka, Russia, and Turkey as the top five countries affected by denial-of-service attacks in exchange for payment, double extortion, and trojan viruses.

Computer and mobile-enabled fraud proliferated in 2020 forcing organizations to focus on enhancing fraud detection. Improving fraud detection ranked highest with 69% of respondents indicating this would be a focus for 2021. The US reported fraud losses of $124 million by mid-2020 and the UK reported 5-10% fraud linked to furlough schemes and over £1.5 billion lost to benefit fraud. Hong Kong also reported fraud losses indicating that HK$1.52 billion of losses were linked to fraud in the first half of 2020.

Interestingly enough, when asked if their organization combines cyber, fraud, and AML, 40.6% said yes. 2021 will continue to see a more rapid convergence between fraud, cybercrime, and money laundering that should be explored further. The early 2020s will prove to be a decisive period, pushing firms to remain vigilant across cyber, fraud, and money laundering as the world eagerly anticipates the mass distribution of COVID-19 vaccines and recovery from the pandemic.

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

ComplyAdvantage: The State of Financial Crime 2021



Combination of responses ranked first, second and third

Firms will need to remain vigilant and fine-tune controls to identify computer-enabled crimes as well as Covid-19-related frauds. However, Covid-19 frauds can vary widely. They can include the sale of non-compliant personal protection equipment (PPE), counterfeit products and test kits, vaccines, and other treatments. They can also include identity theft, investment frauds, crypto Ponzi schemes, online romance scams, social media, social engineering and online shopping, online loans, and fake online jobs all requiring victims to disclose bank account details.

Those examples go beyond Covid-19. Firms will need to screen for and monitor many predicate offenses as many of those examples existed before Covid-19 and will exist after. Fraud, cybercrime, tax crime, and corruption are all ranked highly as the most important predicate offenses for organizations to screen against. Push payment fraud and unauthorized remote banking fraud will also remain a major risk for individuals and businesses. Businesses operating in the medical supplies and pharmaceutical sectors, which are currently very profitable, will become major targets for organized criminals.

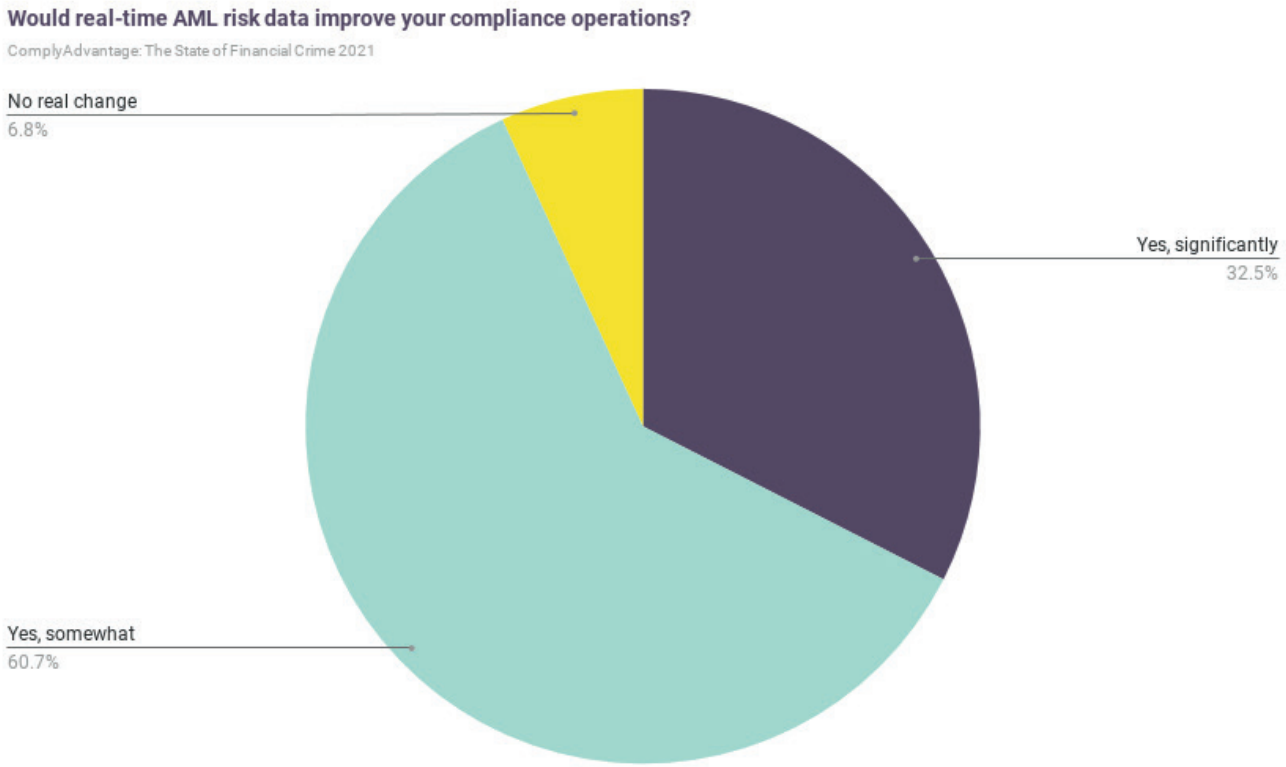
What does this mean for my business?

Where they are not already doing so, firms will need to work closely with governments to identify and report Covid-19-related fraud. They will need to explore how to configure their transaction monitoring systems to identify payments linked to fraudulent activity and cyber-enabled crime and provide customers with the right information to prevent them from falling prey to these types of crimes. Firms will also need to screen fraud and cyber-related crimes when onboarding and throughout the relationship. Monitoring will be an important tool as organizations fine tune their risk-based approach. Adverse Media and Negative News solutions with categories like fraud-linked, cybercrime, property, and financial AML/CFT will prove valuable for managing risk.

Sanctions

Sanctions will remain a key foreign policy and national security tool in the US, while the UK will look to further develop its autonomous sanctions toolkit after Brexit. In the first few days of 2021, the UK already issued 131 removals and 2,172 new updates / data points to their sanctions regime. Protecting human rights will become a significant objective for sanctions regimes. In December 2020, the EU adopted a global human rights sanctions regime, focused on creating comprehensive financial restrictions against individuals and entities involved in human rights abuses, and other jurisdictions, including Australia, are likely to enact similar regimes in the coming year. Countries will also use sanctions to target the abuse of technology, such as state-led cyber-attacks, the use of encryption software, and misuse of crypto wallets to finance terrorism. There may be additional designations linked to the use of biological and chemical weapons. Key hotspots will include Hong Kong, Iran, Libya, Syria, Venezuela, and North Korea; and the world will see an increased use of export controls being implemented. Sanctions may also be used in innovative ways to deal with challenges presented by Russia and China, powerful state actors that may issue tit-for-tat sanctions. The evolving use of sanctions and the increased scrutiny from regulators will likely force organizations to assess the rate at which their data is updated and their ability to act on the insights, an issue reflected in our survey. Conclusively, 93% of respondents stated that real-time financial crime risk data would improve their compliance operations.

In the US, the Office of Foreign Assets Control (OFAC) will continue its work designating individuals and entities as the new administration sets its foreign policy objectives; however, the pace of listing and delisting is likely to decrease following the arrival of the incoming Biden administration. The Global Magnitsky Act will continue to be used as a sanctioning tool to put pressure on corrupt public officials, their enablers, and those responsible for human rights abuses. The new administration is expected to maintain focus on Iran, Syria, North Korea, and Venezuela. Although a slightly less aggressive stance may be taken towards Iran with the arrival of the more conciliatory Biden administration. If the Iranian administration takes a step back from breaching the enrichment and other provisions of the Joint Comprehensive Plan of Action (JCPOA), the US may feel able to rejoin as a result.



The US will also continue to impose trade embargoes and export restrictions through the Bureau of Industry and Security (BIS), with a particular focus on China, Russia, and Venezuela. BIS will turn its attention to emerging technologies, similar to the sanctions imposed on artificial intelligence software automating geospatial imagery analysis announced in January 2020. The US has also listed and delisted numerous vessels linked to the Venezuela oil trade, affecting shipping companies, insurance companies, flag registries, and port operations. These companies will need to continue to assess sanctions risk exposure. On the counterterrorism and cyber front, the US will continue to make use of its counterterrorism and cyber sanctions programs as new threats emerge. Meanwhile, a strategic review of sanctions operations carried out under the new administration may lead to numerous de-listings as well as the removal of the controversial designation of International Criminal Court Chief Prosecutor Fatou Bensouda who was investigating the US for possible war crimes in Afghanistan. Pending approval from Congress, Sudan will be taken off the State Sponsors of Terror list.

At the regional level, the EU will look to add names to its recently launched Human Rights sanctions regime, which had no designations by the end of 2020 and will continue to pool together and issue sanctions against actors it considers harmful to EU policy and security. In 2020, sanctions were issued against Russian actors linked to malicious cyber-attacks on the German Parliament and other EU members. The EU also sanctioned President Lukashenko of Belarus and several of his government's senior officials following controversial elections. Sanctions were similarly issued against several recently appointed ministers in Syria due to the violent repression against the Syrian people. The EU may impose sanctions on Turkey for re-opening Varosha, the disputed ghost town in Turkey-occupied Cyprus. If there is an incident that requires a strong EU response, further sanctions could be imposed under its ISIL Da'esh and Al-Qaeda, Venezuela, Syria, and Ukraine sanctions programs.

Brexit will have an impact on the sanctions regimes of the UK and EU, leading to some divergences in policy, even if overall strategic objectives remain broadly the same. There will be differences in the targeting and timing of sanctions, and while it is anticipated that most EU listings will be transferred across into UK law, there is a possibility that not all will meet the UK's legal test.

The UK will issue further autonomous sanctions to align with its own foreign policy and national security goals, particularly under its hallmark autonomous Global Human Rights sanctions regime. The UK will also release its Anti-Corruption sanctions in 2021. It remains uncertain whether the EU will make much traction in developing its own anti-corruption sanctions, given the political challenges of gaining agreement between 27 member states, some of which have historic economic interests in 'high risk' jurisdictions that might be affected.

In practice, this seems to suggest that the UK is likely to act more broadly and quickly than the EU. This was evidenced even by the end of 2020, with the UK sanctioning 65 individuals and three entities for human rights violations that are not designated by the EU. Furthermore, it took over a month after the UK sanctioned Belarusian President Alexander Lukashenko in concert with Canada for the EU to introduce its own sanctions against the President.

At a global level, the UN will continue to lead sanctions implementation at the international level. Areas of focus will include counter-terrorism via its ISIL and Al Qaeda and Taliban programs and proliferation of weapons of mass destruction. The UN may also issue a handful of additions under its country sanctions programs, including the Central Africa Republic, Libya, the Democratic Republic of Congo, South Sudan, etc. There has been a trend towards delisting persons and entities designated under the Iraq sanctions program which could continue. The UN may initiate joint action on Yemen and Ethiopia if conflicts intensify.

What does this mean for my business?

Given the speed with which sanctions designations are added and removed, it is essential that firms use reputable adverse media and sanctions data providers to screen their customer base (both at onboarding and on an on-going basis) and transactions in real-time where possible. This will support their ability to prevent sanctions breaches and will allow firms to quickly identify any bad actors linked to corruption, tax evasion, or other financial crimes. Firms operating outside of the US should also ensure that they have clearly identified any US personnel working for them and deliver additional, tailored sanctions training given the extraterritorial nature of US sanctions. Firms should also remain mindful of the EU Blocking statute which protects those operating in the EU in "lawful international trade and/or movement of capital" from the extra-territorial application of sanctions laws in third countries, such as the US.

Crypto and Virtual Assets Service Providers (VASPs)

By the end of 2020, the price of Bitcoin had reached $28,888 (now over $35,000) and the crypto market cap was valued at over $550 billion. 92% of organizations appeared positive about their technology meeting or exceeding regulatory requirements, a sign that the crypto market is maturing. But as the value of crypto and virtual assets continues to rally, regulators around the world will work to manage risks and educate consumers. This includes expanding standards and implementing new regulations. By mid-2020, 35 out of 54 FATF members had legally adopted the revised standards with three banning VASPs and 32 introducing regulations. 2021 will see more jurisdictions adopt the revised standards while the crypto assets industry matures and implements AML/CFT obligations more widely.

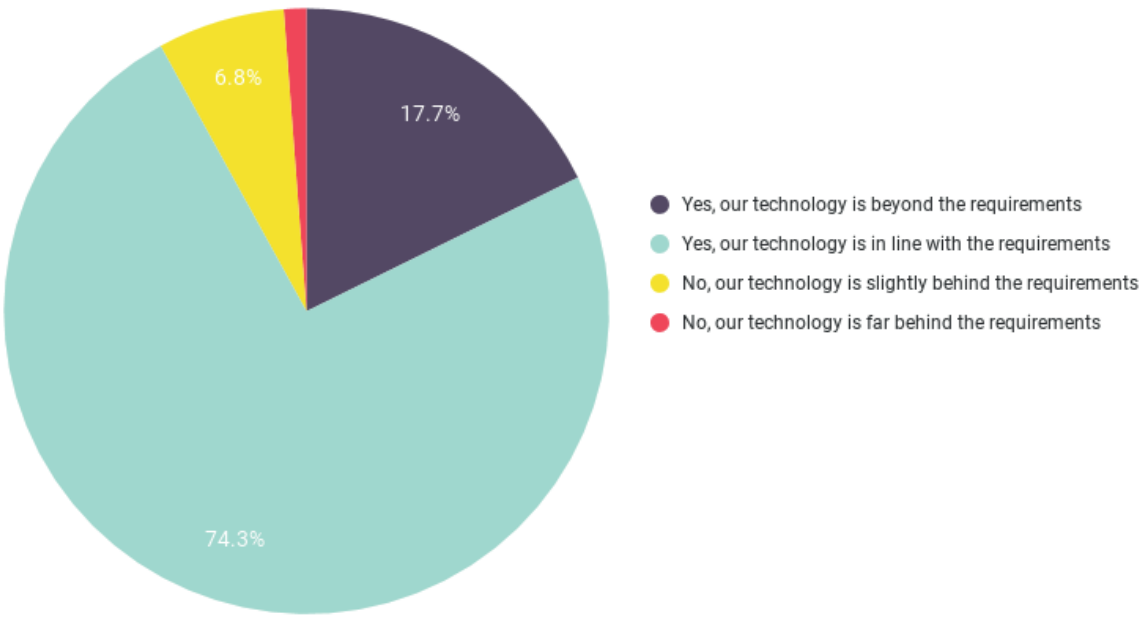
More jurisdictions will adopt licensing regimes for VASPs and regulators will look to expand the scope of regulation beyond custody to include decentralized finance (DeFi), stablecoins, and peer-to-peer transactions. The InterVASPs Messaging Standards (IVMS), a standardized data schema, was issued in 2020 to facilitate the sharing of information to comply with the Travel Rule. This schema will continue to be adopted by the industry as regulators focus on the crypto industry. Many hope that more technology solutions will go live to allow firms to comply with the Travel Rule in 2021.

The FATF has also put other stablecoins, peer-to-peer transactions, and DeFi on notice, indicating that DeFi will likely be brought into scope under AML/CFT regulation. The FATF will also be issuing an update to its Risk-Based Approach to Virtual Assets Service Providers.

And, while some regulators have adopted a nurturing attitude towards VASPs, consumer protection concerns will remain. For example, the UK regulator issued a ban on crypto derivatives trading and the US remains wary. A consultation on proposed rules introducing a licensing regime for VASPs in Hong Kong will close on January 31, 2021. The regime will aim to regulate all virtual asset trading platforms, which currently can opt-in. The Singapore Markets Authority (MAS) proposed a new Omnibus Act for the Financial Sector that would regulate Singapore crypto firms that conduct business overseas and prohibit unsuitable companies from offering their services in Singapore.

Do you feel your organization's technology is able to meet your country's regulatory requirements regarding cryptocurrencies?

ComplyAdvantage: The State of Financial Crime 2021



In the area of enforcement, the industry is likely to see more punitive measures, including past actions. The US charged an individual for operating the bitcoin Helix "mixer" or "tumbler" on the darknet that was used to launder $300 million. The owner was charged with money laundering and operating a money transmission business without a license, effectively defining a "mixer" or "tumbler" as a money transmitting business, which could have licensing implications. The outcome of the BitMex action by US authorities will set a precedent for the ability of exchanges to offer services to firms located overseas. The initial action by the US authorities alleged that BitMEX took on US customers without a license and also breached the Banking Secrecy Act (BSA) by failing to have an effective AML/CFT program in place to manage and mitigate risks.

The crypto industry will continue to upskill itself in matters of AML/CFT and work with regulators to create a greater understanding of risks and technology challenges to AML/CFT implementation. This may also be the year that Facebook's Libra, recently shrouded in mystery, goes live.

What does this mean for my business?

Virtual Asset Service Providers (VASPs) should ensure that they properly assess if they require an operating license for a jurisdiction in which they provide services to or from as new regulation is introduced. VASPs should ensure that they can understand and communicate the risks posed by their businesses as they develop their AML/CFT programs. Firms that wish to do business with VASPs should also ensure that they understand the risks of doing business, carry out adequate customer due diligence (CDD) checks, possibly including understanding the systems and controls in place to manage AML/CFT risks, company culture, and attitudes to compliance, and have the appropriate tools to monitor value transfers. Appropriate training should also be provided to teams responsible for bringing in and on-boarding VASPs as clients.

Terrorist Financing

The terrorist financing landscape is unlikely to change significantly, however, terrorists are increasingly adopting new technologies to finance their operations while still relying on more traditional terrorist financing methods. Europe will continue to be plagued by Islamic terrorism linked to lone-wolf attacks using knives and small arms, such as the recent attacks that took place in Austria, France, and Germany. France, which was the site of several high-profile terrorist acts in late 2020, will face more challenges from homegrown Islamic radicalization. Several countries, particularly the US, the UK, and Germany, will see a further rise in right-wing extremism as nationalist sentiment caused by economic instability takes root. Boko Haram will continue carrying out larger-scale attacks led by smaller cells in West Africa indiscriminately targeting civilians across Nigeria, Niger, Cameroon, and Chad. Al-Shabaab and Islamic State (IS)/Da'esh will remain active in Somalia and East Africa, while Pakistan and Afghanistan continue to be plagued by bombings, mass shootings, suicide bombers, and attacks by the IS/Da'esh and the Taliban. The Philippines will also continue to see terrorist and insurgency activities linked to the Moro conflict in the Mindanao region of the country.

With regards to terrorist financing, as people continue to work remotely, there will be a rise in fraud-enabled terrorist financing. This is facilitated by non-face-to-face onboarding techniques as well as online applications and customer interactions that can easily be manipulated. Techniques previously seen include identity theft, fraud in personal loan applications, bank and insurance fraud, as well as credit card fraud. Mortgage and student loan fraud are also known fundraising sources for terrorist groups. As economic support is issued for the pandemic, it is also likely that this will lead to an increase in benefit fraud. Terrorists will are likely to exploit the Covid-19 pandemic to continue raising funds. In 2020, an ISIS facilitator who manages hacking operations masterminded a scheme to sell fake personal protective equipment. The goods were purportedly sold via an official-looking website and Facebook was used to divert traffic to the malicious site.

The mass adoption of computers and mobile devices will further boost the use of cryptoassets to raise funds and new forms of social networking terrorist financing. A recent US case revealed how the al-Qassam Brigades used social networking sites to request funds and uploaded "how to" videos encouraging the use of Bitcoin to make 'anonymous' donations. Over 150 accounts were tracked and seized by US authorities. In August 2020, the US Justice Department announced that it confiscated $2 million from cryptocurrency accounts used by IS/Da'esh and Al-Qaeda to finance operations. As part of the seizure, more than 300 cryptocurrency accounts were seized and authorities shut down four websites and four Facebook pages linked to the fundraising plot. Al-Qaeda has used encrypted mobile communications app Telegram to manage its money laundering operations, triggering obfuscation techniques to layer transactions.

Terrorist groups may also increasingly adopt methods used by organized crime networks to finance terrorism, including through reinvestment of funds and the use of intermediaries. The UN recently found that Somalia's Al Shabab moved over $1.7 million through one account held in a Somali bank in a 10-week period, which appeared to have been set up to receive zakat, an obligatory almsgiving to support charity. Al Shabab, which had an estimated expenditure budget of $21 million in 2019, also appears to be investing in businesses and real estate while extorting protection payments from businesses. The US recently sanctioned an Australian financier of Al-Qaeda who used his gemstone businesses in Brazil, Sri Lanka, Colombia, Tanzania, Turkey, and the Gulf to launder terrorist funds.

What does this mean for my business?

Given the difficulty in identifying terrorist funds which often start as legitimate funds, firms should identify the terrorist financing risks to their business based on products and jurisdictional risk. Firms should then focus efforts on payments to and from countries identified as having high levels of terrorism activity. Where local terrorist sanctions lists exist, these should be incorporated into sanctions screening at onboarding, payment filtering, and on an on-going basis as a standard. In the event of a local terrorist incident, firms should have in place mechanisms to allow them to quickly respond to and work with law enforcement and regulators to identify and report suspicious transactions and accounts linked to terrorist acts. As terrorists exploit the use of technology, firms should consider how to enhance due diligence measures, including Adverse Media / Negative News monitoring as part of CDD, applying the risk-based approach, and introducing crypto monitoring solutions.

05

Trends in Geopolitics & Impact on Financial Crime

Geopolitics will continue to have a significant impact on financial crime. Although governments have to work together to manage the world's response to COVID-19, countries are likely to embrace nationalist sentiment as they try to boost their local economies. This could lead to events that trigger sanctions as a foreign policy tool, and the world could see heightened levels of criminality that go with economic uncertainty. Key trends to look out for include the inauguration of President-elect Joe Biden in the US, on-going tensions between the West with Russia, Brexit, the rise of China, and political unrest across Africa, the Middle East, Latin America, and Asia as the economic impacts of the pandemic materialize.

Impact of Biden Election

President-elect Biden's ascension to the White House will see the US renew alliances as the US looks to resume its leadership role on the world stage. Having led efforts against corruption and kleptocracies during the Obama administration, it is anticipated that Biden will put anti-corruption and countering illicit financial flows at the top of his agenda. The US government will likely continue to target perpetrators of human rights violations and corrupt persons under its Global Magnitsky sanctions program. In the Spring of 2020, Biden wrote that if elected, he "will lead efforts internationally to bring transparency to the global financial system, go after illicit tax havens, seize stolen assets, and make it more difficult for leaders who steal from their people to hide behind anonymous front companies." This indicates that the world may see the US leading, introducing or moving forward coalitions and initiatives in these different areas.

Sanctions will remain a primary foreign policy tool for the US, however, the number of designations made will not match the record number issued under President Trump. Biden is expected to review sanctions operations to prevent the misuse of sanctions. It is anticipated that Biden will take a softer stance on Iran, looking to rejoin the Joint Comprehensive Plan of Action (JCPOA) nuclear accord or at the very least, reassess sanctions introduced by the Trump administration against Iran. Targeted sanctions will remain in North Korea and Syria as the Biden administration contemplates US policy, and there is an expectation that Sudan will be removed from the State Sponsors of Terrorism list if Congress approves a deal that would see victims of terrorist attacks compensated and pave the way for Sudan to normalize relations with Israel and the US. Biden will also look to address the situation in Venezuela by using 'intelligent sanctions', among other measures. As cryptocurrency adoption grows, more crypto wallet addresses will be listed under sanctions and cyber-crime sanctions will be used to tackle state-led malicious hacks.

What does this mean for my business?

As Biden takes on the US Presidency, firms should be on the look-out for new measures that are introduced or removed as the US looks to re-set many of its policies. Firms should remain alert to large-scale reform in the US and global initiatives that may affect their business as Biden moves forward with his pledge to tackle corruption.

Tensions between the West and Russia

The EU and the US will continue to contend with Russia's destabilizing effects into 2021. Russia is heavily involved in the sale of arms and military engagements in Asia, Africa, Latin America, and the Middle East. Russia will continue to engage in new forms of warfare, using unorthodox tools such as chemical weapons and cyberattacks, and will continue to be involved in proxy wars around the world. This will see Western governments coordinate, including the swift use of sanctions designations targeting senior figures in the Kremlin and the Russian business elite. The poisoning of Russian Opposition Leader Alexei Navalny has led to the UK and EU sanctioning six individuals, including the Head of the FSB, Russia's internal security agency, Deputy Ministers of Defense, and an entity that develops chemical warfare agents. The torture and death in custody of Russian lawyer, Sergei Magnitsky, led to the development of human rights sanctions regimes in the US, Canada, the UK, and most recently the EU, with Australia likely to join in 2021. Arms embargoes, including those placed on dual-use items, and licensing requirements around the sale, export, supply, or transfer of energy and oil-related goods with Russia will not be lifted. And any further Russian interference in Belarus, Ukraine, or neighboring states is likely to be met by German-led demands for sanctions.

US President-elect Biden will need to address Russian meddling in US electoral processes, Russian disinformation campaigns, and Russian interference in US politics using cyber tools and hacking into federal agencies. This will likely lead to better coordination on sanctions with other nations and it is anticipated that there will be more US-European cooperation to counter Russia's influence. In October 2020, Russian entities were sanctioned under the EU Cyber sanctions regime for the 2015 attacks on the German Parliament while the US also recently designated the Russian Government Research Institute and Russian nationals for carrying out phishing campaigns in 2020. If the Russian state launches more cyberattacks with tools recently stolen from top cybersecurity firm FireEye, which has several government clients, it is likely to face additional sanctions by the US, UK, and EU.

What does this mean for my business?

Firms should monitor payments to and from Russia and other CIS member states or entities beneficially owned or controlled by business associates and family members of Russian PEPs. Transactions going to or from Russia should be identified as a higher risk to assess any suspicious payments that could potentially be linked to arms sales and to guard against breaching trade embargoes.

Brexit

In the short to medium term, as the UK and EU move forward after tense discussions surrounding the Brexit Trade Agreement, the parties are likely to stay broadly aligned to the EU on AML/CFT. According to 'Part 3, Title X' of the UK–EU Trade and Cooperation Agreement, published on December 24, 2020, both sides have not only committed to supporting FATF standards, but also to go beyond FATF with the transparency of beneficial corporate ownership and the maintenance of ownership registries. Although the UK will not directly implement the 6th Anti-Money Laundering Directive (6AMLD), UK national laws in many ways already conform to the directive's requirements, with some exceptions, such as the absence of an offense of corporate failure to prevent economic crime, a key change included in the 6AMLD, Nonetheless, this issue will continue to be debated in the UK Parliament, and the UK and EU may yet align on the issue.

Challenges around alignment are more likely to emerge in the medium to long term, mainly due to the differing priorities of the EU and UK. The EU will be concentrating on further regulatory harmonization of national AML/CFT frameworks to address deficiencies highlighted by the 2017–18 Nordic–Baltic Banking Scandals, while the UK is likely to explore how it can push forward the government's vision of a "global Britain." It is this latter objective that is likely to become one of the most contentious areas, with some in EU institutions already foreseeing AML/CFT as one area where the UK might seek to lower standards to under-cut the EU in the future.

As a result of this, and despite the basic similarities of the UK and EU regimes, this lack of trust has so far led to the absence of mutually recognized equivalence on AML/CFT regimes, with real practical implications for compliance teams. Although neither side is defining the other as a 'high risk' jurisdiction, necessitating Enhanced Due Diligence (EDD), firms on either side of the divide are required to consider EU or UK clients as existing in 'Third Countries', bringing additional compliance burdens. This means, for example, that a UK firm onboarding an EU client would need not only to undertake AML/CFT rules based on UK law as before but also know the laws and regulations of the jurisdiction in which the client was based, assess whether they are commensurate or tougher than UK law and if so, ensure that it meets those requirements as well as those of UK law.

This of course would also work in reverse, with EU companies operating in the UK needing to follow UK law in addition to their own. It may be worth noting that the UK government may introduce a financial crime levy on approximately 90,000 regulated businesses that could be liable for payment to raise £100 million annually to support the government's fight against economic crime. The levy is anticipated in 2022 or 2023, but if introduced, this would be the first of its type across the world.

In practice, the kind of impact this will have is unclear. Although for the time being, it seems likely to increase administrative friction for compliance teams. Discussions are ongoing between the EU and UK about several areas of regulatory equivalence that can be agreed upon for the financial services industry, with a 'Memorandum of Understanding' to be issued by March 2021. Compliance officers should therefore keep a close watch on how these discussions develop.

A further area of potential divergence is sanctions. As noted above, the UK has already started making additional designations to those on EU lists, suggesting that in time, the UK will likely introduce measures that they would have previously had a challenge bringing forward within the EU environment. Whether this will lead to a radical divergence of approach seems unlikely however as long as the UK continues to share similar geopolitical concerns and objectives with the EU.

The UK will look to expand its area of influence in other parts of the world as it continues to develop its economic crime agenda and illicit finance networks in major financial centers such as Kenya, Dubai, New York, and Hong Kong. The opportunity for regulatory arbitrage may arise, but it is anticipated that regulators and law enforcement agencies will need to define new ways of working for the better good. However, there may be differing opinions on how to manage financial crime risks in new areas for consideration, such as emerging technologies, free ports, and decentralized finance (DeFi).

What does this mean for my business?

Firms that have not already done so, particularly those headquartered in the EU with UK operations and vice versa, should ensure that their AML/CFT frameworks and programs can monitor and incorporate regulatory changes in both the EU and UK. This includes subscribing to both the UK as well as EU sanctions lists with their data providers. Firms should also integrate both UK and EU national risk assessments into their policies. Firms should also look to both country and region to identify best practices in AML/CFT, particularly as the world embraces technological innovation in AML/CFT and data protection. And finally, regulated businesses in the UK may wish to begin to understand how the financial crime levy would work and assess any potential impact on future budgets.

The Rise of China

China continues to forge ahead as one of the largest economies in the world, moving ahead with its own AML/CFT measures while proliferating financial crime risks as it challenges US global dominance. China recently held the FATF Presidency and will continue to strengthen its AML/CFT framework and report back to the FATF in October 2021. President Xi has also made the fight against corruption a priority; public reporting in 2020 indicated that the Chinese government charged over 18,000 people under its domestic corruption laws in 2019 (twice the amount charged in 2018) and that between 2014 and June 2020, Chinese authorities recovered RMB19 billion (US$D2.8 billion) in criminal proceeds and repatriated 7,831 individuals from 120 countries overseas linked to corruption.

China recently completed a pilot and is in the lead for creating the first working Central Bank Digital Currency (CBDC) to replace cash in circulation, which would boost its monitoring capabilities over the yuan. This would allow the government to better understand Chinese money flows and help track illicit fund flows linked to online gambling, money laundering, and terror financing. This could also support China's objective of making the yuan the primary international currency, a challenge to US dollar supremacy.

China's Belt and Road Initiative (BRI), the development of a modern-day "Silk Road" trade route which is expected to cost US$1 trillion, has been marred by allegations of corruption. The BRI will likely make China the world's biggest foreign investor and creditor as it supports projects in over 70 countries. There are concerns that the Chinese government is militarizing the BRI, with several infrastructure projects in Pakistan, Sri Lanka, and Djibouti connected to the Chinese military. There have also been many scandals linking the BRI to organized crime groups, the rise of private military contractors, bribery of local officials, environmental degradation, and other secret deals. However, the Chinese government recently publicly disassociated itself from a contentious crime-riddled project in Myanmar that was linked with the BRI.

Indeed, China's ability to inflict economic pain is great and it will continue to block foreign direct investment decisions based on national security concerns — as many countries have done regarding Huawei and its 5G technology. This has been an ongoing trend in China's responses to criticisms on its human rights record in the Xinjiang Uyghur Autonomous Region (XUAR) and Hong Kong, its military exercises in the South China Sea — one of the world's busiest and resource-rich waterways, as well as the question of Taiwanese independence.

Against this backdrop, countries will carefully navigate how to respond to Chinese human rights violations. Following criticisms of its human rights record, China triggered a trade war with Australia, putting in place unofficial bans on importing coal, barely, wine, beef among other Australian exports, which will continue into 2021. Among the list of infractions include the use of high-tech state surveillance, censorship, persecution of ethnic and religious minorities, and mistreatment of workers. Western allies accuse China of using facial-recognition technology, a region-wide biometric database, and mobile tracking apps to identify over one million Uyghur and other Muslims in XUAR for forceful "re-education" in detention centers. The US has imposed sanctions on senior officials in China's ruling party in XUAR and blacklisted eleven Chinese companies linked to human rights abuses as well as restricting exports. Other countries may likely follow suit in 2021.

The US also issued sanctions in response to the implementation of the National Security Law in Hong Kong which it claims denies freedom of expression, promotes state surveillance and is likely to lead to violent crackdowns against pro-democracy protesters in Hong Kong. The US sanctioned several Chinese officials linked to the current situation in Hong Kong; and it is likely that the UK and Canada, whose leaders have issued strong condemnations against Chinese actions in Hong Kong, may consider issuing sanctions too. It is anticipated that countries around the world will look to other financial measures to hold Beijing accountable for its poor human rights records.

China also recently introduced its own unreliable entities sanctions regime to prohibit foreign entities from conducting trade and business in China. The Chinese Unreliable Entities List is a punitive list that specifically targets foreign entities that: (1) endanger Chinese sovereignty, security or development interests; and (2) suspends transactions with Chinese corporates or individuals violating internationally accepted economic and trade rules, damaging the legitimate rights and interests of that corporate or individual. The list was announced following a US government move to ban popular social media apps published by Chinese tech giants ByteDance and Tencent.

China has also announced export controls for commercial data encryption equipment and software effective January 2021. These measures have been implemented largely in response to the US–China Trade war in which the US has been adding pressure on China and the rise of big tech. US firms now require licenses to sell Huawei semiconductors made abroad with US technology, and there are over 135 Huawei companies blacklisted under US export controls following espionage claims and allegations of breaching Iranian sanctions. An Executive Order will come into play in January 2021 in the US, prohibiting security investments in companies that finance Communist Chinese Military companies.

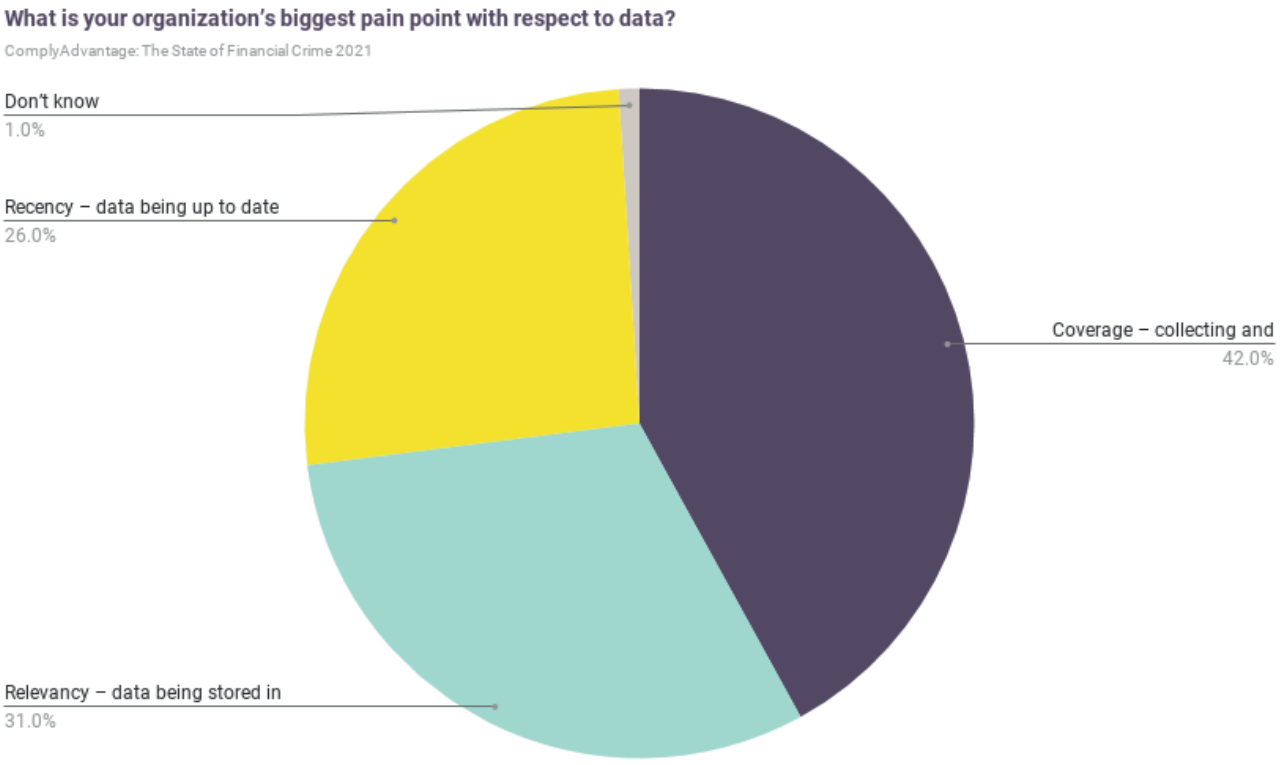
Although the Biden administration will look to develop its foreign policy on China, it is clear that bipartisan support exists for taking a strong stance against Beijing and protecting domestic businesses in the US. The rise of China continues to present situations where the rife use of sanctions could continue into 2021, creating challenges for global businesses.

What does this mean for my business?

Given the rise of the Chinese yuan and the pending launch of its digital currency using eWallets and QR codes, firms may need to consider whether they can monitor payments to and from digital wallets, and identify the risks associated with payments using QR codes. Given the risks of sanctions against and by China, firms should frequently screen their Chinese customers to identify any trade embargoes or human rights sanctions designations. Likewise, firms with Chinese operations will need to ensure that they comply not only with international sanctions, but also Chinese sanctions and trade embargoes put in place as processing any payments could constitute both a sanctions breach and a money laundering offense. Firms offering wholesale banking and trade finance products should also consider carrying out transactional and human rights due diligence on its Chinese–linked customers.

Political Unrest and OCGs

As people begin to feel the economic impacts of the pandemic, political discord is likely to create an arena for malicious actors and organized crime groups (OCGs) to play a bigger role in society. There are countries where the governance systems in place are unable to support effective responses due to mismanagement and corruption, creating highly volatile environments that can be exploited. Countries identified as having extremely high political and security risks in the Americas include Brazil, Bolivia, Chile, Honduras, and Venezuela. Countries in Africa include Burundi, CAR, Ethiopia, Mali, South Sudan, Somalia. In the Middle East, higher risk countries include Afghanistan, Libya, Palestinian Territories, Syria, and Yemen. In Europe, parts of Ukraine remain high risk. These countries tend to be characterized by informal economies, corruption, human rights abuses, and economic inequality, where illicit economies thrive, and bad actors act with impunity. These countries also tend to act as source countries for money laundering and at times, destination countries for terrorist financing. Incomplete or inaccurate data handicaps organizations' ability to assess these threats within their institutions. Coverage remained the biggest pain point with respect to data followed by relevancy and recency.



Countries plagued by political unrest tend to create an environment where organized crime groups can flourish. As traditional sources of revenue such as drugs and trafficking of illegal goods and humans continue to be disrupted, OCGs will continue to diversify and take advantage of poor governance, exploiting the pandemic in a variety of ways. OCGs will issue loans targeting companies in sectors under distress, such as retail marketplaces, hospitality, transportation, arts, entertainment, recreation, and tourism, They will also continue to infiltrate sectors that prove to be lucrative such as the wholesale trade in medical and pharmaceuticals, e-commerce and logistics, and funeral, cleaning, and waste management services. A recent Interpol global operation resulted in the seizure of over four million potentially dangerous pharmaceuticals valued at more than $14 million, involving 37 OCGs across 90 countries. Where governments are unable to support their societies, OCGs will look to enhance their standing and roles in local communities to expand control. They will continue to hand out essential goods and groceries to bolster their local power and influence. In Mexico, OCGs have been distributing basic supplies to businesses and individuals. At the same time, they have been asking for "contributions" from local businesses to finance aid. In Afghanistan, the Taliban sent teams to remote areas to help tackle Covid-19. In Syria, militant group Hayat Tahrir al-Sham disseminated health information; and in South Africa, gangs in Cape Town handed out parcels with food during a short-lived truce.

What does this mean for my business?

Firms need to remain aware of changing trends in financial crime. While many of the aforementioned countries are not listed on the FATF's list of non-cooperative countries and jurisdictions, firms should label them as a higher risk for money laundering. This will allow them to automatically trigger enhanced due diligence on onboarding, but also enhanced monitoring on payments to or originating from countries suffering from significant political unrest. Firms should avoid de-risking but rather speak with regulators and governments for guidance on how to manage payments from higher-risk countries. Firms should particularly be on the lookout for capital flight following political unrest, the laundering of vast quantities of assets, and should particularly look closely at related party transactions where links have been identified to politically exposed persons, including via family members and their enablers. Firms should also be aware that there may be a possibility of sanctions being issued by the US, Canada, the UK, and Australia where gross human rights violations are identified.

06

Regulatory Change and Enforcement

By December 2020, AML fines totaled over US$10.3 billion, and sanctions fines totaled US$25.9 million. APAC saw an upsurge in fines from US$6.6 million in 2019 to US$5.1 billion in 2020, with the Malaysian Securities Commission handing out the largest fine linked to the 1MDB scandal. With the US introducing higher penalties for AML/CFT failures under the NDAA, Europe pledging to impose credible deterrence, and China issuing a record number of fines, the upward trend in fines and regulatory action will continue.

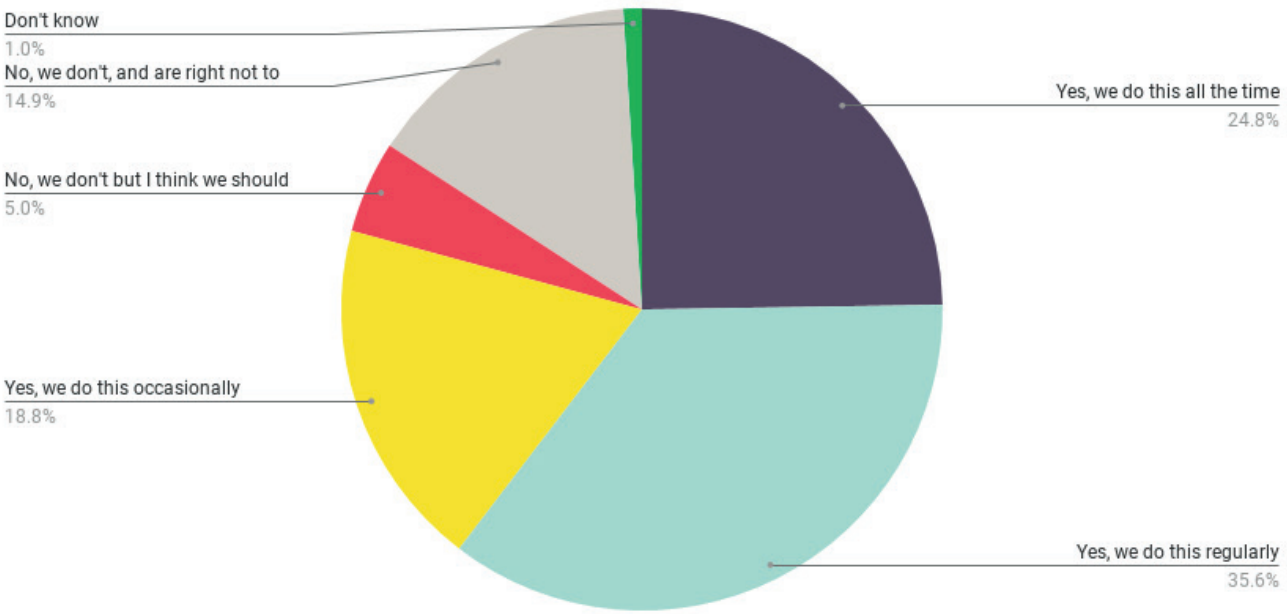
Given the amount of focus the world is placing on financial crime, enforcement actions and fines levied are likely to increase as firms continue to be sanctioned for repeat failures. Changes in regulations paired with increased scrutiny from examiners will force difficult conversations at the c-suite level. A look at the numbers:

- 86% of respondents felt that their organization has the right tools to detect financial crime
- 66% of respondents felt that their organization was investing the right amount in compliance operations and 20% felt that they had more than they need
- 81% of respondents stated that on average their organization performs company-wide risk assessments at least once a year
- 97% of respondents consider the risk of anti-money laundering fines and violations
- 62% of respondents admit to regularly choosing to incur AML fines and make violations

These numbers shed light on the complicated world of anti-financial crime where compliance is seen as a cost center and leaderships' obligations are to their shareholders, employees, and customers. Only 19% of respondents felt that AML regulations needed to be strengthened, but those that did state that AML regulations needed: larger fines for AML violations, personal liability for C-suite, SARs reform, Adverse Media / Negative News requirements, and stronger ultimate beneficial ownership. Significant regulatory changes will take place at the international, regional, and national levels as countries vow to make AML/CFT frameworks more effective, and the value of fines and regulatory activity increases; organizations will need to balance regulatory scrutiny and their risk-based approach.

Does your organization regularly consider the risk and choose to incur anti-money laundering fines and violations with respect to your business decisions and compliance investment?

ComplyAdvantage: The State of Financial Crime 2021



Global

The FATF will continue to steer the international AML/CFT agenda in 2021 and drive forward digital adoption in this space. As part of the Chinese Presidency over 2019–2020, the FATF began a strategic review of its mutual assessment process of country effectiveness for global AML/CFT standards. A new methodology will be published in 2021 to make the process both timelier and more risk-based. Although the FATF has postponed the mutual evaluation assessments of numerous countries due to COVID-19, the FATF continues to work with countries on its grey list and will determine which countries should be added to or removed from its lists that detail high-risk jurisdictions subject to a call for action ("blacklist") or jurisdictions under increased monitoring ("grey list"). The FATF also recently updated its 40 Recommendations requiring the identification and assessment of risks relating to proliferation financing sanctions.

Under the incoming German Presidency, 2021 will see the FATF publish guidance on risk-based supervision and continue its work in the virtual assets space, extend its work on illegal wildlife trafficking to cover other environmental crimes, and harness the power of new technologies to fight financial crime. The FATF has also identified illicit arms trafficking, and the financing of ethnically and racially motivated terrorism, and migrant smuggling as areas of priority until June 2023. The FATF continues to work with VASPs as they develop solutions to comply with originator and beneficiary requirements for transactions under the 'Travel Rule' and will issue updated guidance to the risk-based approach to VASPs. The FATF is widening its efforts beyond decentralized exchanges and custody to focus on stablecoins, peer-to-peer transactions, and decentralized finance (DEFi).

In the area of illegal wildlife and environmental crime, the FATF has begun assessing money laundering risks linked to crimes such as illegal logging, environmental degradation, and waste dumping, among others, and will continue meeting with the not-for-profit and private sectors to define an approach and publish its findings.

The FATF has also touched upon the area of digital transformation during its recently issued COVID-19 paper and Guide to Digital ID. Both documents show a shift in approach to embracing the use of technology as non-face-to-face onboarding becomes the norm and the world increasingly carries out payments and transactions online. 2021 may see the development of more digital identity programs at the country-level and the industry will see increased adoption of RegTech solutions by regulated entities and SupTech solutions by regulators.

What does this mean for my business?

Firms will need to build proliferation financing into their business-wide risk assessments to place appropriate mitigants to avoid unwittingly becoming part of proliferation financing networks and schemes. Firms are likely to see more supervisory visits and fines and should have in place a system and controls inventory to allow them to quickly respond to regulatory requests. DeFi providers should prepare for falling within the scope of AML/CFT regulation.

Firms should also review the FATF's guidance that is published to ensure that they are aware of the requirements of adopting new technologies. They should update their systems and controls, including policies, processes, and IT systems with risk indicators relevant to their businesses. Firms should also build in review and assessment of the FATF's documents as part of their horizon scanning activities as this will allow them preparation time to comply with changes to domestic AML/CFT regulations and regulatory expectations as they trickle down from the FATF.

North America

Three key events will lead to many changes in the US AML/CFT legal and regulatory landscape in the coming years. In anticipation of the FinCEN leaks, the US issued a well-received Advanced Notice of Proposed Rulemaking (ANPRM) on Money Laundering Effectiveness. FinCEN also issued a final rule enacting s.352, s.326, and s.312 of the USA PATRIOT Act closing a major gap in the implementation of AML/CFT standards in the banking sector. At the tail end of 2020, the US House of Representatives and Senate subsequently passed the National Defense Authorization Act (NDAA) 2021 that included the Anti-Money Laundering Act of 2020 (AMLA), which will herald extensive AML/CFT reforms in the US. The NDAA was passed into law on January 1 when the US Senate voted to override President Trump's veto.

In the ANPRM, FinCEN indicated it would develop and communicate national AML priorities and promote the responsible use of innovation to address evolving risks. FinCEN further raised the need for regulated entities to complete AML/CFT business-wide risk assessments, carry out assurance testing, and on-going monitoring of record-keeping and suspicious reporting requirements. The ANPR specifically called out the need for designated entities to provide useful information to government authorities when submitting SARs.

The final rule issued by FinCEN enacting the PATRIOT Act provisions will require banks that lack a Federal functional regulator to adopt customer identification and beneficial ownership requirements. These banks, including private banks, non-federally instituted banks, and some trust companies, were previously exempt. The final rule closed a major gap between state and federally-chartered banks that exposed the US financial system to illicit finance. It will require these banks to set up customer due diligence policies and procedures and effective AML/CFT programs by March 15, 2021.

The AMLA, published after the ANPRM, includes numerous provisions on making the fight against AML/CFT more effective mandating change at both national and entity-level and contains five key sections. The first focuses on strengthening financial intelligence and AML/CFT programs. This includes bolstering FinCEN, improving financial intelligence sharing between agencies both at the domestic and international levels, establishing national exam and supervision priorities, and extending the application of the Bank Secrecy Act (BSA) to dealers in antiquities and assessing its application to art dealers within one year. The Act requires national priorities to be established and made public 180 days after the Act has passed and will be updated every 4 years.

The second section deals with modernizing the AML/CFT system, including encouraging technological innovation and the adoption of technology in reporting. The Treasury will convene a global multi-stakeholder tech symposium to determine how to use technology to promote international collaboration in combating financial crime. This will place a focus on enhancing SARs requirements and law enforcement feedback on SARs, piloting a program on sharing SARs data within a financial group, reviewing currency transaction reports and SARs thresholds, greater sharing of threat patterns and trends, and boosting information sharing and public-private partnerships. The Director of FinCEN will provide a brief on the status of implementation and the use of various technologies, including digital ID and AI, within 90 days of enacting the Act.

The third section of the NDAA provides an overview of how the US will enhance AML/CFT communication, oversight, and processes. This will include improved inter-agency coordination, developing, and training resources, and updating whistleblower protection and incentives. Additional damages for repeat offenders will be levied — three times the profit gained or lost due to the violation or twice the maximum penalty — and individuals could be banned from serving on Boards.

The fourth section relates to the creation of a national beneficial ownership registry, dubbed the "Corporate Transparency Act." The US will issue uniform beneficial ownership information reporting requirements. The collection of beneficial ownership information will be carried out at the federal level. This is being implemented to allow the US to meet its international obligations and to discourage the use of shell companies to protect US national interest. Beneficial ownership information has been classified as "sensitive information" and will only be available to government authorities. This information, however, can be used to confirm beneficial ownership information to allow financial institutions to comply with AML/CFT requirements. A "secure, non-public database" will be established at FinCEN. Reporting entities will have two years to submit beneficial ownership information and submit any changes within one year of those changes.

The final section indicates that the US government will be carrying out numerous studies. These include studies on beneficial ownership reporting requirements, feedback loops to regulated entities, trafficking, trade-based money laundering and proposed strategies, money laundering by China including identifying risks and the effects of illicit finance, efforts by authoritarian regimes to exploit the US financial system, and the effectiveness of currency transaction reporting to law enforcement. The NDAA will also expand the definition of funds in the BSA to include "currency, funds, or value that substitutes for currency," with a nod to capturing cryptocurrency actors.

In Canada, several amendments were proposed to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the PCMLTFA). Amendments include giving greater powers to the FIU, including allowing it to recover compliance costs and widen its ability to disclose additional information, and increasing penalties for money laundering offenses. It will also bring armored car vehicles into scope for regulation and strengthen the regulatory framework for money service businesses.

What does this mean for my business?

Given the significant volume of changes being imminently brought into law by the US, firms should begin identifying which parts of their AML/CFT programs will be affected. A gap analysis should be carried out to assess the impact and adequate costs set aside in future budgets to allow for the right projects, time and resourcing so that organizations can adequately affect change within set timelines. Firms should be prepared to feed into the planned studies where possible as these could impact national policy, but firms also take the findings of the studies and build these into their policies where relevant. Where needed, nominated functions responsible for submitting SARs should receive additional training to ensure that they are submitting useful information and review systems that automatically file SARs to ensure that they are submitting only adequate information. Firms may wish to consider investing in new technologies such as Natural Language Processing to augment information held. Firms that are being newly caught by AML/CFT laws and regulations should ensure that they have the right staff with relevant expertise to build their new AML/CFT programs to allow them to comply.

Europe

2021 will see significant changes in the EU with the introduction of the 6AMLD. Member states are required to transpose 6AMLD into national law by December 3, 2021, and implement it by June 3, 2021. Key changes include the harmonization of 22 predicate offenses for money laundering, including cybercrime, environmental crime, and insider trading, as well as the expansion of criminal liability. For the first time, companies and their members of the Board could be subject to criminal prosecution as the 6AMLD extends criminal liability to legal persons failing to have effective AML/CFT systems and controls in place to manage financial crime risks. The 6AMLD increases the minimum requirements for a prison sentence for money laundering from one to four years, and gives judges the power to fine individuals and impose professional disqualifications as part of the EU's commitment for stricter, dissuasive enforcement, and to ensure that potential 'enablers' of money laundering offenses in the legal and accountancy professions are also covered.

The European Commission (EC), the EU's bureaucracy, is scheduled to make annual reports on the progress of the directive's implementation over the coming years, but past experience suggests that progress will require encouragement in certain jurisdictions. In July 2020, the European Court of Justice (ECJ) fined Ireland €2 million and Romania €3 million for failing to implement the 4th Money Laundering Directive and the EC has already referred Austria, Belgium, and the Netherlands to the ECJ for failure to implement the 5th MLD. Cyprus has also been put on notice and may be referred to the ECJ in January 2021.

In the face of the slow implementation of past directives and following various banking scandals that have rocked Europe, the EU has decided to find ways to harmonize and supervise the region's response to AML/CFT more tightly. In May 2020, the European Commission issued an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, which indicated it would deliver more granular proposals for the effective implementation of existing rules, a single EU rulebook, a new EU-level AML/CFT supervisory function, possibly under the umbrella of the European Banking Authority (EBA), and a cooperation mechanism for the region's financial intelligence units in early 2021.

The EBA is increasingly taking a leading role in developing AML/CFT policy and as of January 2020 became solely responsible for leading, coordinating, and monitoring AML/CFT efforts across the EU financial sector. Following public consultation, the EBA will publish its revised Risk Factor Guidelines for ML/TF in 2021 on how firms should carry out business-wide risk assessments and customer risk assessments. It will also include guidance on the implementation of CDD measures, record keeping, training, and reviewing effectiveness. The draft Guidelines developed guidance on enhanced due diligence linked to high-risk third countries, and industry-specific guidance on crowdfunding platforms, corporate finance, payment initiation services providers (PISPs), account information services providers (AISPs), and currency exchange offices. The Guidelines included additional risk factors linked to terrorist financing, identification of beneficial owners, the use of new technologies to carry out CDD and sets out clear regulatory expectations for businesses' ML/TF risk assessments. The EBA will also carry out a pilot using an updated methodology to develop its ML/TF supranational risk assessment and will likely publish the results sometime in 2021. The EBA is also due to review the list of obliged entities in the scope of AML/CFT regulations. It has indicated that other types of virtual asset service providers, investment firms, and investment funds may be brought into the scope of the AML/CFT framework and further consultations are likely to take place.

What does this mean for my business?

Any firms operating within the EU will need to ensure that they have effective AML/CFT policies and processes in place and commitments from senior management to ensure that they do not fall foul of corporate failure to prevent offenses. When developing AML/CFT training, firms should look to cover the links between various predicate offenses and money laundering to help employees identify and report suspicious behavior that may previously have been overlooked. Firms with cross-European operations must ensure that they have AML/CFT policies in place that comply with the 6AMLD even if they are headquartered in any of the countries fined or referred to the ECJ.

Firms will need to carry out a gap analysis to understand areas for improvement to comply with the Risk Factor Guidelines. Firms will also need to ensure that they update their business-wide and customer risk assessments when the various risk indicators are finalized by the EU and more detailed guidance issued. Entities such as different types of virtual asset service providers, investment firms, and investment funds will need to consider developing AML/CFT frameworks including having individuals in their compliance departments with the relevant knowledge and experience to establish effective AML/CFT frameworks.

Asia—Pacific

Several regulatory developments are brewing in Asia–Pacific this year. Hong Kong and Singapore remain important financial centers driving innovation, taking a more forward–leaning approach to RegTech and issuing guidance on the adoption of technology. Hong Kong has already issued licenses to eight virtual banks and the regulator in Singapore, the Monetary Authority of Singapore (MAS), is one of the most innovative regulators in the world. As key financial centers, they will continue to remain susceptible to money laundering as illustrated by the $1.5 billion – $2.4 billion that transited through Singapore and $1.4 billion – $2.7 billion that transited through Hong Kong revealed by the FinCEN files. Meanwhile, Australia has implemented an AML/CFT Bill, which could deliver regulatory costs savings of up to AU$1.3 billion, and has one of the world's most innovative public–private partnerships. And, while ASEAN countries are looking to have a more unified approach, jurisdictions are moving at their own pace.

Singapore will be assessing firms against new legal requirements and guidance introduced by MAS. The Government introduced amendments to the Payment Services Act (PS Act) to expand the scope of AML/CFT requirements to providers of digital token services overseas, including stablecoins, and improve the framework for managing technology risks. MAS issued guidance setting out supervisory expectations on enterprise–wide risk assessments, effective AML/CFT controls in private banking and strengthening oversight of AML/CFT outsourcing arrangements. MAS also released two separate sets of Guidelines first for variable capital companies on preventing AML/CFT, including provisions on assessing risks with new technologies and payment methods, and then for digital payment token service providers detailing how to comply with AML/CFT requirements. MAS will also continue to work within the Veritas consortium — "the first industry–wide collaboration to provide a mathematical way to validate AIDA solutions against the principles of Fairness, Ethics, Accountability and Transparency" — to encourage the responsible adoption of AI and data analytics (AIDA) by financial institutions.

Several developments will continue in Australia: the country's Anti–Money Laundering and Counter–Terrorism Financing Amendment and Other Legislation Bill 2019 (AML/CTF Bill) passed the Senate in December. However, the amendment extending AML/CFT measures to capture non–financial businesses and professions such as real estate agents, accountants, lawyers was removed. The Bill will strengthen Australia's capabilities to tackle illicit finance and includes changes to correspondent banking obligations, expands the ability of firms to rely on CDD carried out by 3rd parties, adds exemptions to the prohibitions in place around the "tipping off" offense, increases civil penalties for failing to comply with cross–border movement reporting obligations and promotes financial intelligence sharing. On the operational side, Australia's Financial Intelligence Unit, AUSTRAC, will continue to innovate and develop intelligence reports. It will be issuing eight money laundering and terrorist financing risk assessments in the coming years including four on the banking sector, two on remittances, and two on the gambling sector given the risks identified with junket tour operations. AUSTRAC and the Fintel Alliance, the country's public–private partnership, will also continue to work on the Alerting Project due to finish June 30, 2022. To date, AUSTRAC has developed "a world–first algorithm" to allow the Fintel Alliance to protect the privacy of source data while detecting crime. In the sanctions space, the Australian Parliamentary Committee recommended that Australia issue its own Magnitsky–style sanctions to target human rights abusers and beneficiaries of corruption, which is expected in 2021. It is noteworthy that while 65% of respondents noted their use off–shore remediation, Australia surpassed all other countries with 82% using off–shore remediation. As these regulatory changes move forward, it will be interesting to watch how Australian financial institutions and fintechs invest their resources.

Hong Kong released several circulars and guidance documents following the FATF's assessment of its AML/CFT framework which will enhance effectiveness. The Hong Kong Monetary Authority (HKMA) published an updated Guidance on Anti-Money Laundering and Counter-Financing of Terrorism (For Stored Value Facility Licensees). The Guidance will take effect on July 2, 2021. Key changes include the introduction of a tiered approach to CDD through the adoption of the risk-based approach and direction on adopting technology for remote CDD. Technology will remain a big focus, with Hong Kong continuing to support and explore innovation in AML/CFT. HKMA will implement recommendations in its circular on AML/CFT Supervision in the Age of Digital Innovation. The circular indicates that HKMA should pursue data-driven, proactive, and targeted supervision, develop a tech-friendly talent and culture, and explore the use of Application Programme Interfaces (APIs) and cloud-based technologies to deepen collaboration across the AML/CFT ecosystems. The Hong Kong Securities and Futures Commission (SFC) will also be amending its AML/CFT guidelines to support the adoption of the risk-based approach and help the securities industry manage risks including cross-border correspondent relationships. The SFC proposed a new licensing regime that will require all cryptocurrency trading platforms that operate or target investors in Hong Kong to have a license, develop a registration regime for dealers in precious metals and stones, and will also provide for the use of digital identification schemes to manage risks of non-face-to-face onboarding.

Other countries in the region are working to enhance their AML/CFT frameworks. China remains in enhanced follow-up and will report to the FATF on steps taken to strengthen its AML/CFT framework in October 2021, particularly with regard to bringing designated non-financial businesses into the scope and work around corporate transparency. Japan and New Zealand are currently under review by the FATF and are likely to introduce new measures to address any identified deficiencies.

What does this mean for my business?

Firms operating in the APAC region should ensure that they continue to integrate findings from their horizon scanning activities into policy and procedural updates. Where adoption of new technology is considered or outsourcing of AML/CFT activities, firms may wish to look to the guidance issued by HKMA, AUSTRAC, and MAS to support them in managing risks. Firms that offer cryptocurrency services should ensure that they understand the licensing options and limitations in different countries in Asia-Pacific and be aware of new licensing requirements coming in for entities offering services into or from certain jurisdictions.

07

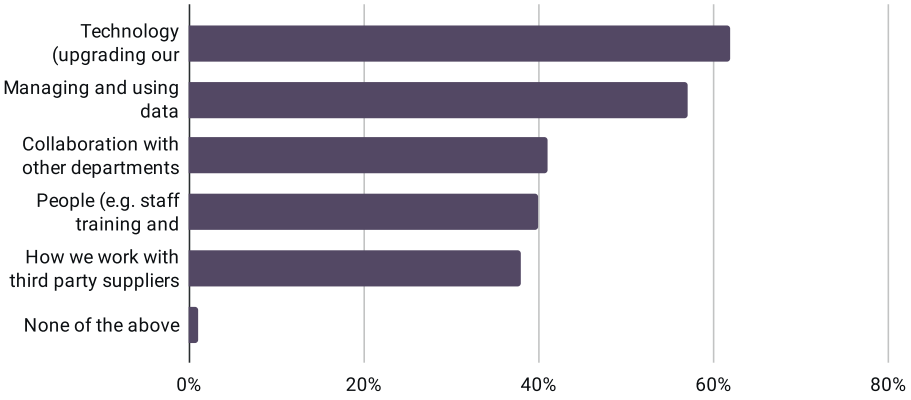
Industry Trends

When asked how prepared their organization would be if they went through a compliance audit today, 89% responded that they would be mostly or completely prepared. Only 11% reported expecting a warning and/or fine. Financial institutions and fintechs will need to remain ahead of evolving regulations and emerging typologies as legacy systems weaken.

Firms and businesses will continue to contend with the lasting impacts of Covid-19 well after 2021. Financial crime compliance and staff will continue to work remotely until normalcy returns and banks will continue to assess how to streamline costs and continue to explore how to adopt technology to increase productivity. Many already have plans to upgrade their legacy systems and improve how they manage and use data in 2021.

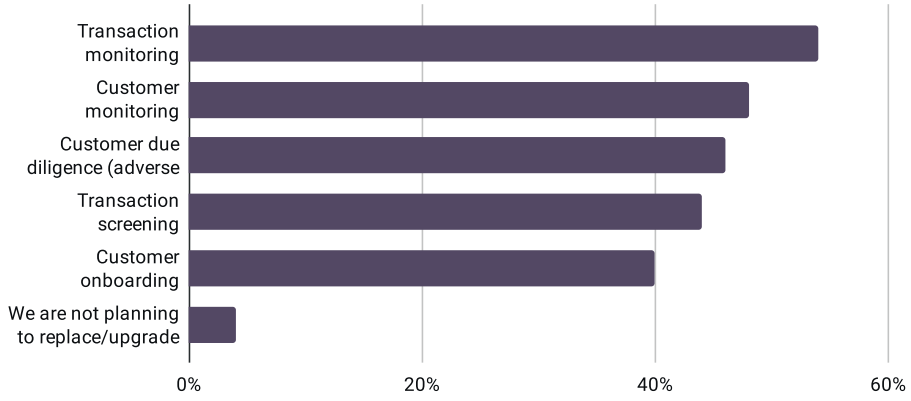
Within your organization's compliance department which areas are you planning on improving in 2021?

ComplyAdvantage: The State of Financial Crime 2021



Which tools are your organization planning on replacing or upgrading in 2021?

ComplyAdvantage: The State of Financial Crime 2021



RegTech Adoption

RegTech adoption will skyrocket in 2021, with COVID-19 accelerating the rate of digitization, and lawmakers and regulators in the UK, Hong Kong, Australia, and Singapore promoting the use of technology to manage risks. The number of digital ID providers and firms that support remote onboarding via the use of biometrics, natural language processing (NLP), and the use of AI and machine learning (ML) to identify and process adverse media and sanctions alerts, is set to rise. However, challenges remain including lengthy sales cycles and the presence of 'black box' solutions that need to be understood and explained. Organizations were asked if they used machine learning, natural language processing, biometric authentication, and or blockchain technology. The result was overwhelmingly positive with respondents using newer technologies with and without vendors.

It is essential that compliance teams have resources in place that can adequately identify risks and communicate to their regulators how their RegTech solutions work. Nevertheless, the HKMA found that 85% of retail banks launched or are planning to launch remote customer onboarding using RegTech solutions and has developed a two-year roadmap to encourage RegTech adoption. The roadmap includes the creation of a "RegTech Knowledge Hub," publication of a "RegTech Adoption Practice Guides," organizing "RegTech Adoption Practice Guides," and includes 16 recommendations to promote RegTech. The UK's Financial Conduct Authority (FCA) also launched a digital sandbox with pilots showing how RegTech can address pressing problems, is regularly hosting RegTech Forum meetings, and launched the Global Financial Innovation Network (GFIN). Australia recently issued a report with recommendations on digital data capture and to promote technological adoption. Its recommendations include the creation of a national digital identity ecosystem, a call to identify how to promote the use of RegTech solutions to support compliance obligations of small and medium-sized enterprises, to study the costs and complexities of FinTechs and RegTechs, hold events to allow FinTechs and RegTechs to "solve policy and service delivery challenges," and re-skill workers impacted by economic changes to allow them to join the FinTech and RegTech industries. There are currently around 1,000 active RegTechs in the world and it is anticipated that the global RegTech market will be worth $55 billion by 2025.

	Machine Learning	Natural Language Processing	Biometric Authentication	Blockchain
Yes, we work with a vendor to provide this exclusively	**28%**	**28%**	**29%**	**30%**
Yes, we do this in-house exclusively	**33%**	**28%**	**31%**	**31%**
Yes, we work with a vendor and do this in-house	**26%**	**25%**	**22%**	**23%**
No, but we plan to in the next year	**8%**	**10%**	**9%**	**11%**
No, but we plan to beyond the next year	**3%**	**4%**	**5%**	**3%**
No and we don't plan to	**2%**	**5%**	**3%**	**2%**
Don't know	**1%**	**1%**	**1%**	**1%**

FinTechs Drive Innovation

FinTechs will continue to drive innovation not just in the offering of financial services, but also in how they manage AML/CFT risks. FinTechs will continue exploring different types of metadata to gain greater insights into customers at onboarding that is not traditionally available or used by incumbent banks. Some FinTechs will also embrace 360 degrees surveillance on customers as opposed to rules-based transaction monitoring to better understand and identify suspicious customer behavior. FinTechs will continue to adopt biometrics to identify customers but also to manage user authentication to prevent financial crime. Lastly, FinTechs will continue to demonstrate how tech and compliance professionals can work together and not only break down functional silos but also how AML/CFT systems and controls can protect customers against fraud. There are several FinTechs that have put fighting financial crime and AML/CFT at the heart of their offering, and this will also allow them to manage risks while addressing de-risking and financial inclusion.

Closer Public-Private Sector Collaboration

There will be closer public-private collaboration to develop initiatives to tackle financial crime, with some countries exploring legislative changes required to make these initiatives more effective. Work will continue to build public-private partnerships, including in Kenya, and countries with existing public-private partnerships (PPPs) like Australia will find them useful in identifying and addressing emerging threats.

The COVID-19 pandemic has provided fertile ground for investigative cooperation in a number of areas. In the space of innovation, regulators will continue to convene TechSprints, bringing together technology firms, banks, regulators, and subject matter experts to develop innovative solutions for specific AML/CFT use cases at both national and global levels, as was seen by the G20 TechSprint. While caution remains around cross-industry data sharing, collaborations such as Transaction Monitoring Netherlands (TMNL) will move forward to develop supranational transaction monitoring with the support of regulators. Given the massive shift to digital onboarding and rising costs of compliance, more progress will be made in establishing KYC utilities. Invidem, a KYC utility set up by six Nordic banks with the go-ahead received from the European Commission, is likely to drive the development of common KYC standards in Europe. Dubai has established a KYC blockchain platform with six other banks, and Abu Dhabi and Singapore are also working on KYC utilities. Identifying non-face-to-face onboarding as lower risk will drive more countries to develop e-ID programs to allow citizens to prove their identity online, creating a golden source of data for IDV.

What does this mean for my business?

Firms should be on the lookout for opportunities to innovate and embrace new solutions in a cautious manner to drive down costs, increase efficiencies, and the effectiveness of financial crime measures.

08

Key Dates in 2021

Q1 – EBA to publish biennial Opinion on AML/CFT Risks

Q1/Q2 – UK to issue anti-corruption sanctions

January

- 1: Brexit
- 1: Launch of UK autonomous sanctions regime post-Brexit

February

- 21–26: FATF Plenary & Working Groups (FATF Events Website) & possible discussion for the following country mutual evaluations: Japan, South Africa, New Zealand

March

- FATF possible discussion for the following country mutual evaluations: Eswatini
- US banks that lacked a Federal functional regulator must set up CDD policies and AML procedures by March 15
- UK government to strengthen the consistency of professional body AML/CTF supervision
- Europol Threat Assessment

April

- FATF possible discussion for the following country mutual evaluations: Egypt, Holy See, Vatican City

May

- FATF possible discussion for the following country mutual evaluations: Guinea Bissau, Grenada

June

- 2–4: UNGASS 2021 – United Nations Special Session of the General Assembly against Corruption
- 3: 6MLD comes into effect in Europe
- 18–23: FATF Plenary & Working Group Meetings
- FATF possible discussion for the following country mutual evaluations: Qatar, France, Indonesia

July

- FATF possible discussion for the following country mutual evaluations: Ecuador, Lao People's Democratic Republic, Nepal, Marshall Islands, Brunei Darussalam, Namibia

August

- FATF possible discussion for the following country mutual evaluations: Namibia

October

- 22–27 — FATF Plenary & Working Group Meetings
- FATF possible discussion for the following country mutual evaluations: Luxembourg, Germany

December

- UK government expected to consider legislative changes to improve the Proceeds of Crime Act 2002
- FATF possible discussion for the following country mutual evaluations: Virgin Islands

September

- FATF possible discussion for the following country mutual evaluations: Poland, Croatia

November

- FATF possible discussion for the following country mutual evaluations: Aruba, Kingdom of the Netherlands, Gambia, Cote d'Ivoire, Palestinian Authority

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 500 enterprises in 75 countries rely on ComplyAdvantage to understand the risk of who they're doing business with through the world's only global, real-time database of people and companies. The company actively identifies tens of thousands of risk events from millions of structured and unstructured data points every single day. ComplyAdvantage has four global hubs located in New York, London, Singapore and Cluj-Napoca and is backed by Ontario Teachers', Index Ventures and Balderton Capital. Learn more at:

complyadvantage.com

Our Customers

Santander VISA OakNorth Bank CURVE

raisin. Munich RE Lydia OANDA

Get in Touch

EMEA
London

+44 20 7834 0252
Demo Request

AMER
New York

+1 (646) 844 0841
Demo Request

APAC
Singapore

+65 6304 3069
Demo Request

ComplyAdvantage