State of Financial Crime 2021

Mid-Year Review

ComplyAdvantage

Contents

01

Summary

The first half of 2021 has been a time of significant change in the world of financial crime. Traditional criminal supply chains continue to be disrupted, with law breakers evolving and entering emerging industries as well as other markets and modes of finance. Change is also being driven by the growing focus of senior policymakers on efforts to combat money laundering and terrorist financing. A strong desire to avoid being placed on a Financial Action Task Force (FATF) blacklist is another incentive in favor of action.

This report will explore the state of financial crime in 2021 so far across three key areas:

- Geopolitics and sanctions
- Regional regulatory trends
- The regulation of cryptocurrencies and innovation in decentralized finance (DeFi)

In **geopolitics**, domestic political unrest and regime change has enabled countries to use sanctions to support their foreign policy objectives. Countries such as the United States are reassessing how sanctions are used, with a growing focus on the promotion of human rights. Meanwhile, others – including China – are increasingly using sanctions as a retaliatory measure. In the UK, the end of the Brexit transition period has allowed the country to launch its own global anti-corruption sanctions program, an early sign of divergence with the European Union (EU). It's clear that sanctions are only going to become more important as a tool of foreign policy in the months ahead.

Across the **regional trends** analyzed in this report, it's clear many countries are prioritizing the fight against illicit finance with the US, EU and China revamping their AML/CFT frameworks. EU member states have scrambled to update their domestic laws ahead of the implementation deadline for the latest anti-money laundering directive (AMLD). The EU has also unveiled a swathe of new legislation including the launch of a supranational AML/CFT authority, and a new AMLD that member states would need to transpose. In the US, regulators have published a number of updates on the implementation of the Anti-Money Laundering Act, including progress towards the creation of a non-public beneficial ownership registry. In the Asia-Pacific region, a lot of change has been driven by Financial Action Task Force (FATF) mutual evaluations at the country level, as well as technological advancements in China, Singapore, the Philippines and Australia.

There has also been much change in both technological innovation and AML/CFT regulation for **crypto firms and virtual asset service providers (VASPs)**. Recent FATF plenary sessions have implications for crypto licensing, and what AML/CFT programs should look like for crypto firms and VASPs. More countries are also bringing forward legislation to implement the travel rule requirement, but significant challenges remain. More widely, FATF has found that there are inadequate safeguards against VASPs being exploited by criminals. In Europe, very few crypto firms met registration requirements, with only a handful of fully regulated firms operating across the UK and EU. In the US, the Office of Foreign Assets Control (OFAC) took action against crypto firms found to have breached sanctions. China is cracking down on its crypto industry, particularly crypto miners, while in Hong Kong, access to crypto exchanges is being limited to professional investors only. Through the rest of 2021 stablecoins will continue to be reviewed, and the wider decentralized finance (DeFi) market will grow further. Many pilot projects are also underway to look at the viability of Central Bank Digital Currencies (CBDCs), with the Caribbean taking the lead in launching CBDCs for use in retail environments.

What does this mean for my organization?

With change continuing at an exponential rate, firms need to ensure they're familiar with emerging regulations, and understand how these will affect their operations. Established institutions must ensure that their systems and controls – including customer due diligence (CDD), know your customer (KYC), onboarding, sanctions, adverse media screening, transaction monitoring and more – remain up-to-date and effective.

Fintechs must ensure that they understand the particular risks they face, and have the right resources in place to continue developing their AML/CFT programs. Firms operating in the crypto space should comply with laws and regulations in the countries they operate in, and make sure they have access to the expertise they need to check they are applying all the measures appropriate to the nature and scope of their business.

Robust technology systems that increase the speed and efficiency with which AML/CFT risks are managed are key. But firms should understand how the systems work, and ensure they are complying with their own internal policies as well. Monitoring legal and regulatory changes, as well as understanding the rationale for fines that are issued, will help with this. Horizon planning remains critical, as will ensuring that staff are adequately trained on emerging risks.

02

Geopolitics and sanctions programs

Biden's sanctions reset

The Trump administration focused heavily on economic sanctions, issuing over 3,900 independent sanctions actions. None of Trump's predecessors had exceeded 700 sanctions actions in a single year. This resulted in thousands of persons and entities being designated and delisted. While not dramatically shifting the United States' overall approach to sanctions, President Biden came to office pledging greater consultation with allies and strategic geopolitical partners.

With this direction in mind, Treasury Secretary Janet Yellen has announced a comprehensive review of sanctions. The objective? To make sanctions a "strong, viable" US national security and foreign policy tool. By coordinating with allies including Canada, the United Kingdom (UK) and the European Union (EU), the administration is seeking to align with its wider focus on democracy and the defense of human rights.

Fall out from China's National Security Law continues

By the time President Bident took office, a number of measures had already been introduced against Hong Kong, including:

1. The Hong Kong Autonomy Act

   The Hong Kong Autonomy Act was issued by Congress in response to China breaching its commitment to allow Hong Kong a 'high degree of autonomy'. This included the unlawful kidnap, arrest and removal from Hong Kong of those seeking to exercise freedom of speech and assembly.

   It allows for the identification and sanctioning of foreign financial institutions (FFIs) that contribute – or attempt to contribute – to China's failures to meet its 'one country, two systems' obligations.

   It also prohibits dealing with designated FFIs, including by making loans available, allowing them to act as a primary dealer of US debt instruments or holding US government funds. It denies US companies the right to complete foreign exchange, banking and property transactions with FFIs. The right to sanction corporate officers, principals and shareholders with a controlling interest is stated as well.

2. Executive Order 13936 on Hong Kong Normalization

   EO 13936 was issued in response to the implementation of the National Security Law which curtailed freedom of expression in Hong Kong, and promoted state surveillance alongside violent crackdowns on pre-democracy groups. Under this EO, several Chinese officials have been sanctioned.

Measures in response to the National Security Law continued after Biden took office. In July, a US Business Advisory was issued targeting US persons and entities operating in Hong Kong. It flags operational, data privacy and electronic surveillance risks linked to the National Security Law. Also in July, a further seven Chinese officials were sanctioned for undermining democracy.

Action against Communist Chinese Military Companies (CCMC) – a broad range of entities allegedly owned or controlled by China's military – has also continued, building on EO13959. Issued in the final months of the Trump administration, it addresses concerns that US capital investments were being used to support the development and modernization of Chinese state military infrastructure.

On June 3rd, Biden issued Executive Order 14032. Taking effect from August 2nd, the EO replaced EO13959, recognizing that additional steps were necessary to combat the nationals security threats China poses to the United States. This includes concern about the use of Chinese surveillance technology outside China, and the development or use of Chinese surveillance technology to facilitate human rights abuses.

EO14032 includes a specific list of CCMCs subject to sanctions, as well as the owners and controllers of sanctioned entities. For those holding securities issued by CCMCs, the EO contains a grace period for divestment of securities June 3, 2022 or 365 days after a company is designated as a CCMC.

G7 responds to China's Belt & Road Initiative (BRI)

At the G7 in June, world leaders launched 'Build Back Better for the World' (B3W). Widely regarded as a response to China's $1 trillion BRI, it focuses on infrastructure development in low/middle income countries with a strategic eye on climate and human rights initiatives. This means that, once developed, it will likely include requirements on due diligence, international sanctions compliance and measures to mitigate corrupt behavior. This is a direct contrast with the BRI which, as we reported in our State of Financial Crime 2021 report, has been marred by allegations of corruption.

BIS Entity List changes for Hong Kong, Myanmar and Russia

The US Commerce Department's Bureau of Industry and Security (BIS) has revised its list of organizations subject to export controls, to align with changes to OFAC sanctions and wider US foreign policy objectives. They key changes included:

- The removal of Hong Kong as a separate destination under Export Administration Regulations (EAR). This means items subject to export controls under EAR – including items destined for use by the military – are now treated as exports, re-exports or transfers to/from China. A number of Hong Kong government entities were also added to the BIS military end-user restricted list.
- The addition of Myanmar to the list of countries subject to export controls for products being distributed for military use.
- The imposition of export controls on Russia in response to the poisoning and imprisonment of Alexei Navalny, a prominent opposition leader. Goods and technologies that could be used to develop chemical and biological weapons were also prohibited.

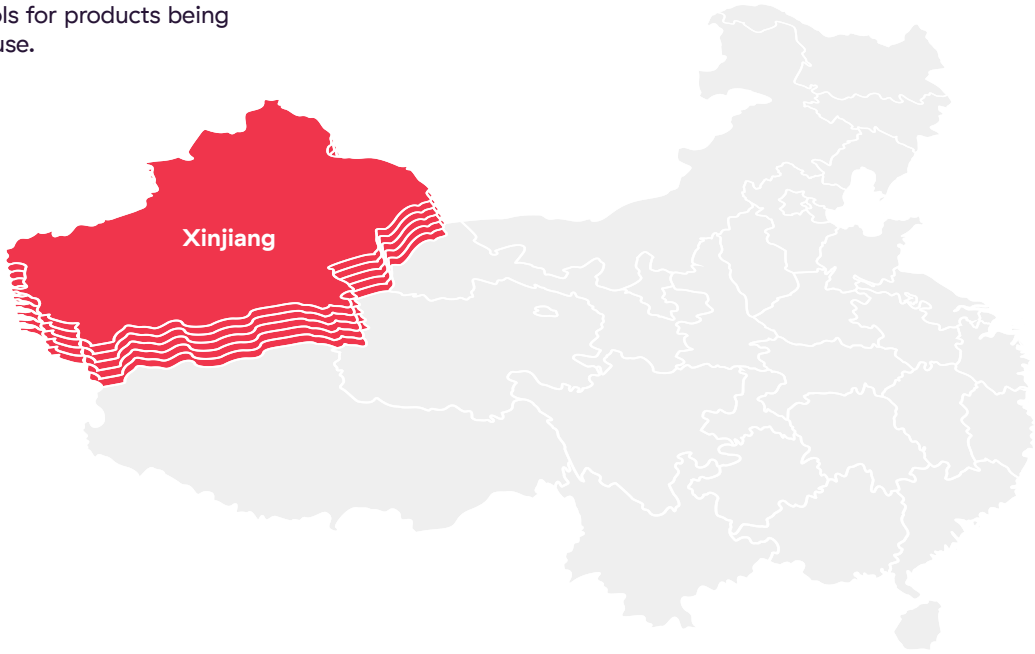
China's dispute with Australia continues to escalate

In 2020, China introduced trade embargoes and other economic sanctions on Australian products. This was a response to criticism by Australian authorities regarding human rights abuses in Xinjiang and Hong Kong. In April 2021, Australia canceled two agreements linked to the BRI. A month later in May, China suspended bilateral dialogue on commerce and economics. Relations deteriorated further in July when a Chinese official indicated directly that "Beijing has singled out Australia for economic punishment" as a result of criticism from Australia on the way Beijing was handling investigations into the origins of COVID-19. Embargoes remain on coal, barely, meat and wine.

Human rights sanctions programs expand

As forecast in our 2021 State of Financial Crime report, this year Australia joined the US, UK, Canada, Latvia, Lithuania and EU in announcing a specific sanctions program to target human rights abuses. These Magnitsky-style laws, named after the original US Magnitsky Act, have enabled increased coordination among countries.

This international coordination was put into practice in March 2021 when coordinated action was taken against four Chinese government officials and a Xinjiang security body for systematic rights violations against Uyghurs and other minority groups. Human rights abuses reported in Xinjiang include mass detention and surveillance, torture and forced sterilization.



The UK's Foreign Secretary stated that: "Acting together sends the clearest possible signal that the international community is united in its condemnation of China's human rights violations in Xinjiang and the need for Beijing to end its discriminatory and oppressive practices in the region."

Other human rights actions taken in 2021 include:

- **The EU acted on North Korea, Libya, Russia, South Sudan, Eritrea:** In March, the EU imposed restrictive measures on individuals and entities responsible for repression in the Democratic People's Republic of Korea. Action was also taken on extrajudicial killings and disappearances in Libya and the torture and repression of LGBTI persons and political opponents in Chechnya, Russia. Finally, sanctions were imposed on South Sudan and Eritrea due to torture and extrajudicial executions.
- **US imposed sanctions on Nicaragua:** In June the US imposed sanctions on Nicaraguan officials under its Magnitsky program for supporting efforts to undermine democracy, human rights and the economy. In August, the European Council adopted asset freezes against eight high profile officials, including Vice President Rosario Murillo.
- **UK sanctioned Myanmar, Pakistan:** In the first half of 2021 the UK also used human rights sanctions to impose measures against Myanmar and Pakistan.

Reviving the Iran nuclear deal

The Biden administration remains focused on reviving the nuclear deal agreed under the Joint Comprehensive Plan of Action (JCPOA). As a first step towards this objective, in February the US rescinded UN sanctions imposed by President Trump against Iran. In June, the US lifted sanctions on around a dozen Iranian officials and energy firms.

However, six rounds of negotiations have ended without a final agreement, with Iran failing to return to the table. There is therefore uncertainty as to whether the JCPOA will move forward, or additional sanctions will be imposed. In particular, there are concerns that, in the two years since the US withdrew from the agreement, Iran has ramped up its production of nuclear fuel. International inspectors have also been barred from accessing facilities. Further doubts remain over terrorist financing and Iran's drone and guided missile programs. The ascension of Ebrahim Raisi, a close ally of the Supreme Leader, to the presidency makes a quick return to the JCPOA still more unlikely.

New measures imposed on Myanmar

Sanctions were reimposed on Myanmar following a February 1st coup by the military, which led to the arrest of religious, government, civil society and human rights leaders, as well as journalists. With E.O. 14014, the Biden administration:

- Froze the assets of persons and entities in the new government.
- Blocked the property of persons operating in the defense sector, as well as those complicit in undermining democracy, security, stability and freedom of assembly.
- Referenced taking action against the spouses and adult children of designated persons.

No change in North Korea

North Korea (Democratic People's Republic of Korea, or DPRK) remains subject to US, United Nations (UN) and other international sanctions. Although no notable new measures were enacted in the first half of 2021, at the G7 in Cornwall leaders issued a statement calling for the denuclearization of the Korean peninsula, and for the DPRK to cease development of weapons of mass destruction, as well as its ballistic missile program. So far however, the US has not designated any additional persons or entities in 2021. Enforcement of existing sanctions measures continues. For example, a Singapore-owned oil tanker delivering oil to North Korea in violation of US sanctions was recently seized.

Broad EU-UK sanctions alignment remains

Post-Brexit, the UK and EU remain generally aligned, with many sanctions programs stemming from EU sanctions regulations. That continued desire to coordinate sanctions policy was evidenced by the actions taken on Xinjiang and Belarus. Moving forward, the EU is likely to focus more on sound, synchronized action across its member states. The only minor discrepancies evident so far have occurred on timing, with the UK sometimes releasing new sanctions designations ahead of the EU.

One area where the UK is acting independently, however, is on its anti-corruptions sanctions program, launched in April 2021. 27 individuals and entities are currently sanctioned for offenses including bribery and the misappropriation of assets. Those targeted in the program so far include:

- 14 individuals involved in a $230 million tax fraud in Russia, perpetrated by an organized crime group, and uncovered by Sergei Magnitsky.
- Three members of the Gupta family for their roles in serious corruption in South Africa.
- Three individuals involved in serious corruption in Honduras, Nicaragua and Guatemala — including facilitating bribes to support a drug trafficking cartel.
- One Sudanese businessman for the misappropriation of significant amounts of state assets in one of the very poorest countries in the world.
- Five individuals involved in serious corruption that have deprived developing countries of vital resources in Equatorial Guinea, Zimbabwe, Venezuela and Iraq.

Coordinated action on Belarus continues

Belarus' increased reliance on anti-democratic activities has continued to prompt a coordinated response from the US and its allies. In June, Canada, the EU, UK and US coordinated sanctions in response to the forced diversion of a Ryanair flight. The flight was rerouted in order to detain a journalist who was onboard. The EU and US also added Russian officials to the Consolidated List for serious human rights violations for their role in the treatment of Navalny, following his criticism of the way elections were conducted in Belarus.

Cuba's political situation deteriorates

During the 2020 presidential election campaign, Biden's team pledged to normalize relations with Cuba. The current political situation in the country makes this unlikely. To help reduce economic pressure, the US is expected to ease restrictions on remittances to Cuba.

Two actions were taken in July under Executive Order (E.O.) 13818 GloMag, which builds on the Global Magnitsky Human Rights Accountability Act aimed at the perpetrators of human rights abuses and corruption. Under the EO, Cuba's Minister of Defense, Special Forces Brigade and the entire Cuban police force were sanctioned. The measures were in response to civil protests against shortages of food and medicine, including attacking, arresting or disappearing protestors in violation of their human rights.

As of July 2021, a review of the United States' Cuba sanctions, the most comprehensive program administered by the Office of Foreign Assets Control (OFAC), is ongoing.

Possible sanctions hotspots to watch

Wherever conflict and political instability go, sanctions may well follow. Here are some of the areas to look out for in the second half of 2021:

- **Afghanistan:** Due to longstanding sanctions against the Taliban, Afghan government reserves held in financial institutions were frozen once it seized power. A number of countries also already have a sanctions program for Afghanistan to comply with UN sanctions – this is primarily related to terrorism concerns. Regulators – such as the Financial Conduct Authority (FCA) in the UK – are also publishing guidance on financial crime risks in Afghanistan.
- **Haiti:** The recent assassination of President Jovenel Moïse has sparked instability and led to a power vacuum in the country.
- **Ethiopia:** The US became the first country to impose sanctions in 2021 due to major human rights violations in the Tigray region.
- **Myanmar:** Following a military coup on February 1st, the political situation within the country is highly unstable. It is also unclear to what extent the new government will be recognized by world powers. US Secretary of State Antony Blinken has accused the security forces of a "reign of terror."
- **Ransomware and cyber:** High profile ransomware attacks like the one on the US Colonial Pipeline have brought this issue to the top of the agenda. US regulator the Financial Crimes Enforcement Network (FinCEN) and OFAC have said that making ransomware payments creates legal risks for victims, banks and insurers. Action must be taken to demonstrate that the recipient is not a sanctioned person.

What should my organization do? Four next steps

With the fast-evolving geopolitical landscape in mind, firms should:

1. Ensure efficient client screening and payment filtering systems are in place so all relevant sanctions lists can be screened against. The exact lists included will depend on where a firm operates, but may include UN, local or regional lists.
2. Understand and explain to regulators the algorithms used by their systems. This includes how systems are calibrated, and ensuring they are conducting regular testing on an ongoing basis to confirm that systems are operating as intended.
3. Hire properly trained staff to manage sanctions risks. This is critical as sanctions become more technical, sectoral and specific to particular industries or products. In particular, expertise is needed in areas judged to be at a high risk of facing sanctions. Firms can then ensure staff have the training required to enable them to better identify sanctions risks.
4. Carry out horizon planning to identify potential new sanctions announcements. These can then be cross-referenced with client portfolios that can be affected, so firms can take action proactively.

To learn more about sanctions, geopolitics and emerging trends, download our report:

The Evolving Use of Sanctions

02

Regional trends

National governments and regulators often take wildly divergent approaches to a host of AML/CFT issues. In this section, we explore the trends that have emerged in countries across the Americas, Europe and Asia Pacific in 2021 so far.

Americas

The Americas region is experiencing the greatest overhaul of AML/CFT legislation in a decade, with the US and Canada implementing new regulations, alongside a sharper focus on beneficial ownership transparency. In Latin America, government positions on the status of cryptocurrencies are becoming clearer.

United States

The US remains committed to implementing the Anti-Money Laundering Act (AMLA). As the country's AML landscape evolves to strengthen its hostility to illicit finance, the US will see a swathe of new regulations and ongoing consultations.

On June 30th FinCEN issued a 180 day update on the implementation of the AMLA. In it, FinCEN states it would "continue to make AML Act implementation a top priority." Over the past six months significant progress has been made:

- February 2021: Plans announced to host an inaugural Financial Crimes Tech Symposium at a future date, meeting a commitment under AMLA Section 6211.
- March 2021: A notice issued on trade in antiquities and art. This followed an update to AMLA Section 6110(a), which amended the Bank Secrecy Act's definition of a "financial institution" to include those "engaged in the trade of antiquities."
- April 2021: An advanced notice of proposed rulemaking on beneficial ownership was published, seeking industry feedback as part of the implementation of the Corporate Transparency Act (CTA, AMC Act Title LXIV, Sections 6401-6403). The CTA amended the BSA to:
  - Introduce reporting requirements around beneficial ownership structures.
  - Create a non-public beneficial ownership register under FinCEN, with information that can only be disclosed under specific circumstances, and to certain recipients.
  - FinCEN also amended CDD/KYC regulations for financial institutions "to take into account the new direct reporting of beneficial ownership information."
  - FinCEN has said it will issue new regulations before January 1st 2022.
- May 2021: New FinCEN subcommittees were launched on innovation and technology, and on information security and confidentiality to address emerging issues.
- June 2021: In response to the no-action letter assessment (AMLA Section 6305), FinCEN determined it would create a process for issuing no-action letters. These are sent to a reporting party by an agency to indicate it will not take enforcement action against the conduct specified in the letter.
- June 30th 2021: National AML/CFT priorities and related guidance were published, in accordance with AMLA Section 6101. Updated every four years, in their first iteration these include corruption, cybercrime, domestic and international terrorist financing, transnational criminal organizations, drug and human trafficking, human smuggling and proliferation financing. The priorities are "intended to assist covered institutions in their AML/CFT efforts and enable those institutions to prioritize the use of their compliance resources."

FinCEN advises firms to take these into consideration alongside the US Treasury's 2020 Illicit Finance Strategy and 2018 National Risk Assessment.

A statement was also issued for banks and non-banking financial institutions clarifying that firms are not required to make changes until FinCEN adopts implementing regulations. However, firms "may wish to start considering" how to feed priorities into their AML/CFT programs, including by carrying out risk assessments on products, services, clients and countries of operation.

FinCEN also appointed Michele Korver as its first Chief Digital Currency Advisor. Her role will be essential in driving "coordinated efforts to maximize FinCEN's contribution" to innovations including in the digital currency space and "minimizing illicit finance risk."

Canada

In June, the final parts of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) came into effect. However, Canada's financial intelligence agency, the Transactions and Reports Analysis Centre of Canada (FINTRAC) has said it will be flexible with new AML requirements until mid-2022.

Enforcement actions in Canada have continued to focus on the housing market. Of the five actions taken so far in 2021, almost all have targeted real estate companies. Real estate and gaming are key focus areas within Canada, particularly in British Columbia, which established a beneficial ownership list in 2020. Domestic orders have also been issued against local terrorist groups, including the Proud Boys.

On June 1st 2021 the changes introduced through the PCMLTFA included:

- Greater beneficial ownership due diligence and transparency.
- Reporting for large virtual currency transactions, and new travel rule requirements (See section 4 on cryptocurrencies for more on the travel rule).
- Increased obligations for foreign money service businesses.
- Greater requirements around prepaid cards.
- An update to the 24-hour rule, which requires the aggregation of multiple transactions totalling $10,000 or more within a 24-hour period.
- Updates to customer screening, ongoing monitoring, record keeping, employee training and CDD/KYC requirements, as well as the onboarding of politically exposed persons (PEPs).

FINTRAC also issued guidance on May 18th that it would "exercise flexibility and reasonable discretion in the course of assessing reporting entities' compliance programs." Compliance assessments against the PCMLTFA will then begin on April 1st 2022. FINTRAC also indicated it would focus on high-risk sectors including "real estate, casinos, financial entities and money services businesses".

Latin America

Mexico

In June the Bank of Mexico issued a statement warning that virtual assets including Bitcoin, Ether and XRP, are not legal tender. It explicitly stated that financial institutions are not authorized to offer services to the public that involve virtual assets including deposits, custody, exchange or transfers. Virtual asset service providers must be authorized, with the country's financial intelligence unit (FIU) announcing in July that 12 crypto exchanges were operating illegally.

In the same month Ricardo Salinas Pliego, the billionaire chairman of Banco Azteca's parent company, announced that he intended to make the bank the first in Mexico to do business in Bitcoin. Mexico's central bank swifty dismissed the announcement, adding it did not intend to change its policy in the foreseeable future.

Salinas Pliego had also been a prominent supporter of a bill designed to compel the central bank to buy back dollars Mexican banks are being forced to hold as a result of US banks reducing the number of bulk cash payments they were accepting from Mexico. This followed an $881m bulk cash shipment scandal involving HSBC, as it transpired these funds originated from drug traffickers.

El Salvador

This year El Salvador became the first country to approve Bitcoin as legal tender. The announcement came into force in early September. It will mean no capital gains tax on Bitcoin transactions, as well as the granting of residency to foreigners who invest three Bitcoins (approximately $120,000) in the country. The move has been met with condemnation internationally and generated local controversy, with protests breaking out over concerns the country will become a "money laundering haven."

To learn more about the latest trends in the Americas, download:

A Guide to the US Anti-Money Laundering Act
Canada: Anti-Money Laundering and Terrorist Financing

Europe

June 3rd 2021 was the implementation deadline for the latest anti-money laundering directive (AMLD), with many EU countries scrambling to pass legislation before the deadline. Further reform continues to be a priority as cracks emerge in existing policies. It also emerged that 2020 was a blockbuster year for AML banking fines, with the total exceeding $200m.

European Union (EU)

In June the European Court of Auditors (ECA) published a report showing that a fragmented AML/CFT approach in Europe is exposing countries to regulatory arbitrage. The ECA recommended that the EU should rely on regulations instead of directives, as these do not need to be transposed at the member state level. It noted that the European Commission has launched infringement procedures against every member state for gaps in the transposition of the 4th AMLD. It has also opened 23 infringements against different member states in relation to the transposition of the 5th AMLD.

A July announcement by the European Commission confirmed that AML/CFT rules will be overhauled to "improve the detection of suspicious transactions and activities, and to close loopholes used by criminals to launder illicit proceeds or finance terrorist activities through the financial system." The changes will also take into account new challenges generated by technological innovation including virtual currencies, integrated financial flows and the cross-border nature of terrorist financing.

The announcement included details on four proposed pieces of legislation:

1. Regulation to create **a new pan-European AML/CFT Authority** to be operational by 2024. The authority will have both direct supervisory powers over high risk financial sector entities, and coordinate the wider non-financial sector. It will also work with FIUs at the member state level on areas including reporting standards. The authority may have both direct and indirect supervisory powers, and could even decide which banks and other financial actors will be subject to direct oversight. It will come into existence on Jan 1st 2023, with its first regulations being applied Jan 1st 2024. On Jan 1st 2026 direct supervision by the new authority will begin.

2. A new AML/CFT regulation to create **a single EU rulebook for all AML/CFT legislation**. Importantly, these rules will not need to be transposed into national law. It will contain rules that are directly applicable and rules on internal policies and customer due diligence. More detail will be added on the type of information needed to identify beneficial owners, including specifying what information to collect, as well as guidance on PEPs and outsourcing.

   A cross-border system to connect national banking registries is also being proposed. This is designed to ensure that FIUs can access information on bank accounts and their owners from across the EU.

   The rulebook will set an EU-wide limit of 10,000 EUR for large cash payments. New obligations on employee integrity, and prohibits the provision of anonymous accounts are also outlined.

   Finally, several additional entities will also become subject to the EU's AML/CFT rules. This includes crypto asset providers, mortgage credit intermediaries, consumer credit providers as well as organizations working to secure residence permits for third-country nationals. Alternative Investment Fund (AIF) and UCITS – collective investment in transferable securities – will also be included.

3. **Proposed language for a new AMLD**. This will be transposed into national law, and amends rules on national supervisors and Financial Intelligence Units in member states, including enhanced supervision and improved intelligence sharing. It will also clarify obligations for home-host supervisors of cross-border transactions. Supervisors will be granted powers to remove a management function and prevent persons not deemed "fit and proper" from holding a registered function. The ability to carry out checks and sanctions for effective beneficial ownership registries will also be introduced.

   The deadline for transposing the new AMLD into national law will be three years from its adoption date. At that point, previous AMLDs will be repeated.

4. Amendments were introduced to the 2015 Regulation on Transfers of Funds (Regulation 2015/847/EU) to ensure it also applies to crypto-asset transfers.

Germany

In March, Germany passed a new AML/CFT law to implement the latest AMLD. This defines new criminal offenses and sanctions that extend beyond the requirements of the legislation. For example, money laundering offenses no longer need to be related to a predicate offense – most of which are committed by gangs, or for commercial profit. It is now sufficient for money laundering to originate from any 'unlawful act' at all. This means that assets derived from even petty offenses such as shoplifting can now also be considered the object of a criminal money laundering offense. Perpetrators can be considered to have intentionally committed money laundering if they consider the money they're handling is derived from an illegal act of any kind. In other words, the perpetrator of money laundering does not have to establish a link to a specific offense. As a result Germany has redefined its conceptualization of money laundering, moving away from a pure focus on tracing profits from serious criminal offenses. In taking this step, it goes beyond the requirements set out by the European Union.

Money laundering committed 'recklessly', i.e. without intent to commit the offense, is also now a punishable offense. A conviction for money laundering is therefore possible if the court is convinced that the perpetrator did not recognize the origin of the assets from an unlawful act, but grossly violated their duty of care when checking the origin of the funds. Frivolous money laundering is punishable by up to two years in prison or a fine.

These changes are expected to significantly increase the number of suspicious activity reports filed in Germany. This reflects the country's desire to use money laundering-related offenses to not just combat serious crime, but also more effectively monitor monetary transfers and payment transactions across the country.

On June 8th, the Federal Financial Supervisory Authority – BaFin – issued new 'interpretative and application' guidance for Germany's Money Laundering Act. The key guidance issued included:

- The assumption of a strongly increased risk of money laundering and terrorist financing related to cash transactions. As a result, credit institutions are now required to observe special due diligence obligations, in addition to those already in place when certain cash limits are exceeded.
- A move to distinguish between cash transactions conducted within 'regular' business relationships, and all other transactions. The guidance sets different thresholds for the due diligence required in each circumstance. For regular business customers, the threshold is 10,000 EUR. Outside of this, 'reasonable measures' must be taken to clarify the origin of assets over 2,500 EUR. Exceptions are included for sectors such as retail, where higher cash transactions occur regularly.
- Tighter money laundering obligations for the real estate market. This includes guidance on circumstances under which the regulator would expect suspicious activity reporting obligations to be triggered. For example, when the purchase price agreed for a property clearly exceeds its market value, or when corporate entities with murky corporate structures – especially with international connections – are involved.
- A broad interpretation of rules stipulating whether investors are to be regarded as beneficial owners of the funds in which they're investing. This is designed to prevent investors from evading identification via indirect participation in funds.

  Guidance on due diligence requirements in correspondent banking relationships. This includes information on group-wide risk assessments and how information is shared. BaFin also highlights when additional due diligence obligations apply. This could include the involvement of PEPs as beneficial owners, or if the residence of a beneficial owner is in a 'high risk' third country.
- On the data processing systems that enable credit institutions to screen and monitor transactions, BaFin sets out both the technical and personnel requirements firms must achieve. It also explains the circumstances under which data processing can be outsourced to third countries. It states that this should only be necessary under very limited circumstances. Final assessments cannot be outsourced.

The intention behind this guidance is to provide more certainty for firms on their legal standing. It is expected that firms will implement the recommendations as soon as possible – only the new cash ceiling includes a two month transitional period.

France

The Autorité des marchés financiers (AMF) – France's national regulator – updated its general regulation and guidelines on AML and CFT to transpose the most recent AMLD, including action on:

- Taking a risk-based approach.
- Due diligence on clients and their beneficial owners.
- PEPs.
- Reporting of suspicious activity reports (SARs) to Tracfin, the country's AML enforcement body.

Updated guidance reminds regulated institutions to assess risks at a country-level, taking into account:

- The list of high-risk jurisdictions or those under surveillance established by the FATF.
- The list of high-risk third countries established by the European Commission in application of Article 9 of Directive (EU) 2015/849 of May 20, 2015.
- The lists published by the OECD and the European Union relating to non-cooperative jurisdictions in tax matters or adopted in application of article 238-0 A of the general tax code.

Finally, the guidance reiterates the need to have a system for detecting atypical transactions based on customer knowledge, in order to:

- Detect suspicious transactions based on a customer's risk profile.
- Process alerts, leading to enhanced analysis and a suspicious activity report if necessary.

The Autorité de contrôle prudentiel et de résolution (ACPR), which supervises the banking and insurance sectors in France, issued a statement in January aimed at protecting French banking and insurance customers from the fallout of Brexit. It 'reminded' UK-based companies that contracts concluded prior to the UK's exit from the EU 'remain valid'. It called out customers with banking and payment accounts, and insurance contracts agreed with a UK insurer as examples. UK firms are encouraged to provide French customers with as much information as possible – and declared that the ACPR will be checking the content of communications sent to French customers.

In the first six months of 2021 the ACPR has also issued sanctions against at least seven financial institutions. Companies sanctioned ranged from banks to payment institutions working across the financial sector, including in insurance, banking operations and crowdfunding. The firms were sanctioned because their AML-CFT procedures, systems and monitoring tools were judged by the ACPR to not be compliant with regulatory requirements.

In July, the ACPR also highlighted the growing number of French firms outsourcing their AML/CFT controls. The authority is particularly concerned that external providers are not properly supervised. It reminded companies that they remain responsible for their compliance obligations, must be able to carry out their controls diligently, and that the ACPR may request direct access to information from an external provider. On-site inspections could even be extended to include contractors.

In addition TRACFIN, France's Financial Intelligence Unit, released a report on financial activity in the country through 2020. It showed an 18 percent increase in the number of SARs sent to TRACFIN by the financial sector. It also listed new money laundering and terrorist financing typologies, including around the use of cryptocurrencies and benefit fraud. The latter increased due to the pandemic.

In March, the French government issued its 'Action Plan against Money Laundering and Terrorist Financing for 2021-2022' giving financial institutions insight into where the country's regulatory landscape will be heading. The five core elements of the plan are:

1. Intensified inspections in both the financial and non-financial sectors.
2. Increased transparency by developing France's beneficial ownership registry, and ensuring it is available to the public.
3. Boosting the powers of TRACFIN to "intercept illicit flows linked to emerging forms of crime."
4. Growing the use of asset freezes as a tool against suspected money laundering, terrorist financing and the purchase of weapons of mass destruction.
5. Enhancing national policies against money laundering, alongside a leading role for France within the EU.

UK

Following the end of the Brexit transition period on December 31st 2020, the Joint Money Laundering Steering Group (JMLSG) – a body made up of trade associations in financial services – issued a statement on the implications for AML/CFT regulated firms. The JMLSG's guidance is critical, because its guidance notes are approved by HM Treasury, and regulators are known to assess against its documents when conducting inspections. The areas called out in its statement include:

- The definition of a 'third country' – any country other than the UK is now a third country for AML/CFT purposes, including entities in the European Economic Area (EEA).
- Correspondent banking – firms should "take cognisance of the effectiveness of the AML/CTF regime of any third country when determining the extent of the EDD measures to apply to respondents in that country."
- Payment service providers (PSPs) are expected to provide the same level of information "regardless of whether funds are being transferred to/from EEA countries or any third country." They should also look at The Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019 and take account of any changes.

In May, the Financial Conduct Authority (FCA) also issued a 'Dear CEO' letter to retail banks on common AML failings – this included expectations around governance, risk assessments, transaction monitoring and suspicious activity reporting. Among the key takeaways, the FCA said it would be taking a more "intrusive" approach to monitoring AML systems and controls. It said it would consider taking action to address weaknesses "even if it is not apparent that these have resulted in the facilitation of financial crime."

In July, the UK government published The Money Laundering and Terrorist Financing (Amendment) (No.2) (High-Risk Countries) Regulations 2021. The legislation updated a list of third countries requiring enhanced due diligence under Schedule 3ZA. At the time of writing, the list includes Albania, Barbados, Botswana, Burkina Faso, Cambodia, Cayman Islands, Democratic People's Republic of Korea, Haiti, Iran, Jamaica, Malta, Mauritius, Morocco, Myanmar, Nicaragua, Pakistan, Panama, Philippines, Senegal, South Sudan, Syria, Uganda, Yemen, Zimbabwe.

HM Treasury also initiated a review into the UK's AML/CFT regulatory and supervisory regime. Open to consultation until October 14th, it is likely to lead to legislative changes in Spring 2022. Its goal is to look at the overall effectiveness of the UK's AML/CFT regime, and understand if regulations on taking a risk-based approach, due diligence and SARs are operating as expected. It will also explore the adequacy of supervision by the FCA and the Office for Professional Body Anti-Money Laundering Supervision (OPBAS), which supervises the legal and accountancy sectors.

Among the reforms being considered are:

- The introduction of an exemption for low risk payment service providers.
- Clarifications to the definitions of a 'financial institution' and 'credit institution'.
- Strengthened supervisory powers.
- The introduction of provisions on proliferation financing.
- The introduction of the formation of limited partnerships under requirements for trust or company service providers.
- The ability to report discrepancies in beneficial ownership on an ongoing basis.
- Enhanced information sharing and gathering.
- The application of the travel rule to crypto assets.

Meanwhile, as the EU presses ahead with its own AML/CFT regime overhaul, we are likely to see more divergence between the UK and EU. While both systems are broadly similar at the moment, one notable difference is in the area of corporate criminal liability for AML/CFT failures. Tougher punishments in this area were brought in with 6AMLD in the EU, which the UK opted out of.

Asia Pacific

2021 has seen a sharper focus on AML/CFT in Asia Pacific. Countries have stepped up their fight against money laundering and terrorist financing with new legislation, amendments and industry guidance. Many of these amendments have been designed to address concerns raised by FATF in countries' mutual evaluations. At the same time, a massive growth in technology-enabled financial services in Asia is generating new risks.

China

The Chinese AML regulatory landscape continues to evolve. In June, new amendments to the Anti-Money Laundering Law were published for public comment by the People's Bank of China. These amendments were designed to:

- Improve the effectiveness of the AML/CFT framework.
- Expand AML obligations to all individuals and organizations.
- Widen definitions of money laundering.
- Increase penalty fines up to CNY 200,000.

Enhanced regulation of non-financial entities. The new rules include requiring trusts to stop making new investments in offshore companies.

Hong Kong

In June 2021, Chinese lawmakers passed the Anti-Foreign Sanctions Law. Many of its components are expected to become law in Hong Kong. The law provides a framework for countering foreign sanctions – particularly those from the United States. It grants China the power to designate foreign individuals, companies, their spouses and relatives if they are seen to be acting against China's interests by complying with foreign sanctions.

The law allows for measures including the denial of visas, asset freezes, and even deportation. Local companies can also sue foreign firms if they're impacted by international companies complying with sanctions on China. The first wave of counter-sanctions targeted seven American individuals and entities, with more expected.

The Anti-Foreign Sanctions Law follows the introduction of the Blocking Statute in January 2021. This requires Chinese companies to inform China's Ministry of Commerce (MOFCOM) when they are forbidden from engaging in economic and trade-related activities due to foreign sanctions.

Australia

Incremental implementation of reforms were agreed under the Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2020 to enhance AML/CFT rules. Compared to the pace of change in other countries, however, Australia is judged to be moving slowly.

In June, Tranche 1.5 reforms came into play, including:

- Changes to customer due diligence, correspondent banking, information sharing and cross-border payment reporting.
- Streamlined due diligence requirements for correspondent banking relationships, and a ban on financial institutions providing services to an institution that permits shell banks to use their accounts.
- Reporting entities are not allowed to provide a designated service until proper customer due diligence is completed.
- Rules around reliance on third-party due diligence are clarified, including specifying cases and circumstances when SARs can be shared with third parties.

Singapore

In March, the Monetary Authority of Singapore (MAS) issued a paper entitled 'Guidance on Strengthening AML/CFT Controls of Digital Payment Token Service Providers'. This provides an overview of MAS' AML/CFT requirements and supervisory expectations for the Digital Payment Token (DPT) sector, with advice on how to establish AML/CFT systems and controls.

In April, MAS announced $42m in grants designed designed to accelerate the adoption of risk management and regulatory compliance technologies in the finance sector. These 'RegTech grants' are available to Singapore-based financial institutions, with funding ranging from S$75,000 to S$300,000.

An Extended Digital Acceleration Grant (DAG) scheme was also boosted with an additional S$30m aimed at supporting the program until December 31st 2021. The DAG is designed to encourage the adoption of digital solutions that enhance productivity, cybersecurity and operational efficiency.

In June, a host of notices were issued by MAS on issues including AML/CFT in banking, payment service providers, digital token payment services, capital market intermediaries and merchant banks. These notices listed AML/CFT requirements, providing guidance on risk assessment, customer due diligence, third party reliance, internal policies and the reporting of suspicious transactions.

Through July and August, MAS ran a consultation on a proposed new AML notice for activities relating to precious stones and metals. This policy is designed to underscore how financial institutions should manage their operations and business activities when dealing with precious stones, metals and products.

United Arab Emirates (UAE)

In the UAE, 2021 has seen a continued focus on tackling illicit finance. In January, the country's central bank announced it had imposed AED 45.76m in fines for AML/CFT control failures. In February, a dedicated body was launched to implement an AML/CFT law passed in 2018. In May, new enforcement rules for violating AML regulations and not registering correctly came into effect – including fines of up to AED 5m. Particular scrutiny is being placed on 'DFNBPs' – a group that includes brokers, real estate agents, auditors, precious goods dealers as well as corporate service providers.

What does this mean for my organization?

Given the host of regulatory changes that are being developed and implemented, it is essential that firms remain aware of what is coming and deadlines for compliance. Firms will need to review each piece of legislation in the countries in which they operate along with guidance issued by the local supervisor, likely conducting an analysis to identify potential gaps against new requirements. Where gaps are identified, firms will need to update their AML/CFT and sanctions policies and procedures in addition to IT systems to ensure that they are operating in line with expectations. This will include CDD/KYC, screening, transaction monitoring, payment filtering and reporting systems. Firms may also wish to engage with vendors to understand if and how they are implementing new requirements into their solutions. Where countries are issuing updated risk assessments or national priorities, it may be worth reviewing business and customer risk assessments and risk indicators in policies that feed these assessments assessments and risk indicators in policies that feed these assessments.

04

Cryptocurrencies and virtual asset service providers (VASPs)

2021 has seen a number of new technological innovations and updates to AML/CFT regulations for VASPs to comply with. One key theme this year is that regulators are increasingly seeing crypto companies as money service businesses (MSBs) and e-money businesses that should be licensed as such. As a result, some organizations are investing in AML products in the expectation that they will be required to get a license, and/or face an audit.

Financial Action Task Force (FATF) Plenary Session guidance on cryptocurrencies

At its June 2021 plenary session FATF, the international standard setter for AML and CFT regulations, reviewed what AML/CFT programs should look like for crypto firms. It also reviewed the implications of these programs for licensing and operating costs.

FATF reported on its second 12-month implementation review of the revised standards on virtual assets and VASPs first set out in 2019. Specifically, the review focused on:

- Implementation at the country level of updated FATF standards on virtual assets.
- Technological advances to support travel rule requirements under Rule 16, which requires originator and beneficiary information to be disclosed on wire transfers.

The review found that 58 jurisdictions now have specific regulations for VASPs, with 52 regulating VASPs, and six banning them. FATF also indicated it will look to provide further guidance on mitigating risks associated with ransomware-related virtual assets, and the ongoing monitoring of peer-to-peer transactions.

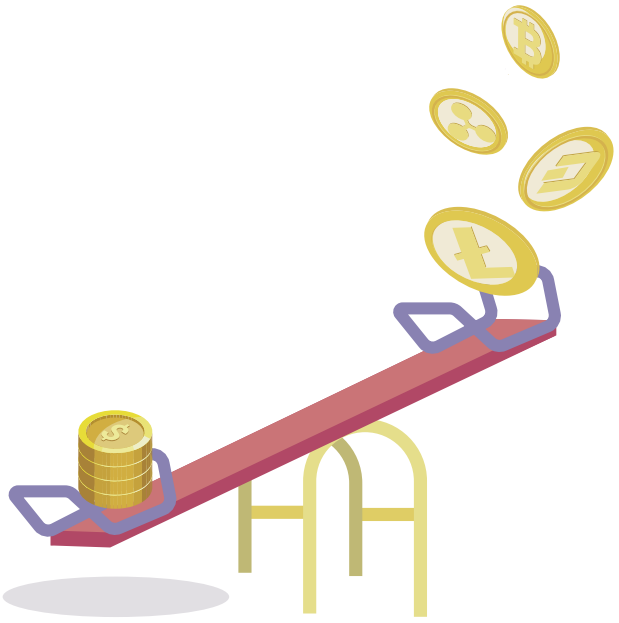
FATF said it will make no further updates to global standards related to VASPs in the short-term, and will issue updated guidance to its risk-based approach to virtual assets in November 2021.

The implementation of FATF guidance will have important implications for licensing and operating costs. VASPs operating in jurisdictions that have adopted national laws to comply with FATF standards must have adequate AML/CFT policies and procedures in place. In jurisdictions that have banned VASPs, notably China, Bolivia, North Macedonia, Vietnam, Iran and Columbia, VASPs must cease operations.

Travel rule implementation review

FATF has been critical that most jurisdictions have so far failed to implement the travel rule, creating risks that VASPs will be used for money laundering and terrorist financing. Just 15 have introduced Travel Rule requirements. In its report, FATF concluded that:

- There is no global framework for Travel Rule compliance.
- No holistic or scalable technological solution exists, with a lack of domestic regulation "acting as a disincentive" to invest in "technology solutions and compliance infrastructure to comply with the travel rule."
- Current safeguards to prevent VASPs from being exploited by criminals are inadequate.



Critically, FATF highlighted that "the lack of a unified technology" solution is undermining travel rule compliance efforts. As a result, companies have adopted both manual and automated processes to submit the information required to comply. Third-party technology solutions were also being used for information sharing, with other VASPs using blockchain-based technologies for information sharing.

Europe: Crypto compliance remains low

Across much of Europe, very few crypto firms have met the registration requirements set out in the Fifth Anti-Money Laundering Directive (5AMLD). This is despite a June 3rd 2021 deadline for countries to put in place VASP requirements, in line with 6AMLD.

In the UK, to date the FCA has only approved nine crypto licenses. The Temporary Registration Regime (TTR) has been extended until March 31st 2022, allowing companies that applied for registration by December 2020 to continue operating while they are being assessed. However, the FCA has noted that an "unprecedented number" of companies are withdrawing their applications, as companies have not met required AML/CFT standards.

Meanwhile Germany, generally seen as a crypto friendly jurisdiction, granted its first crypto authorization in June. In March, Ireland passed legislation requiring crypto asset exchanges to be registered with the Central Bank of Ireland, with an end of July deadline for registrations to be completed.

At the wider EU level, the European Commission announced a proposal to create a regional AML authority, including changes to VASP rules to capture travel rule requirements. The new authority should also oversee international firms that are offering services in Europe. These rule changes are expected to impact how firms are structured when operating in Europe. Among the measured proposed are:

- Expanding "traceability requirements for crypto assets" to comply with the travel rule. This will include defining what personal information will be required for originators and beneficiaries.
- Where companies do not have a branch or head office in a country, they will be required to appoint a central person responsible for establishing AML/CFT programs.

The European Commission has also adopted the Markets in Crypto Assets (MiCA) framework which will harmonize the regulation of crypto assets across the European market while supporting innovation and promoting market integrity. The framework defines which tokens meet the criteria of 'financial instruments' and which meet new 'crypto assets' definitions. It also introduced an 'e-money token' as a type of crypto asset, and covers stablecoins as a 'significant asset-referenced token.'

United States: Treating crypto companies like financial services organizations

In the US, there is a growing consensus that crypto companies offer financial services and/or securities that should be delivered in accordance with existing rules and regulations. As a result, it's increasingly important for crypto companies to put comprehensive compliance and AML/CFT programs in place.

Since 2009, crypto regulation enforcement actions in the US have now reached $2.5bn covering fraud, AML, sanctions breaches and offering securities without a license. In February 2021 OFAC reached a $507k settlement with BitPay, a bitcoin payment service provider, for processing payments for merchants that originated from individuals in China, North Korea, Iran, Sudan, Syria and Crimea. BitPay had access to individual Internet Protocol (IP) addresses which should have alerted it to where the payments were coming from, with OFAC indicating that IP geo-blocking should have been in place. A mitigating factor in BitPay's favor was that it had an active sanctions compliance program in place, including staff training.

In May, the US government announced that crypto assets will be expected to report transactions equivalent to $10,000 to the Internal Revenue Service (IRS). This is designed to prevent tax evasion and ensure compliance with currency transaction reporting rules that apply to other financial services firms under the Bank Secrecy Act.

China: Crackdown on crypto

In May the Chinese government issued an order to "crack down on bitcoin mining and trading behavior." The statement specifically cited "illegal securities activities" as an area of focus.

In June, the government began action against crypto miners, launching whistleblowing programs to allow people to report Bitcoin miners and cracking down on crypto exchanges. A country-wide crypto ban then began in July, with an additional 11 exchanges shut down for "violating foreign exchange rules" and breaching country-wide regulations.

Although financial and payment companies are forbidden from providing crypto-related services, it's worth noting that individuals in China are not yet banned from holding cryptocurrencies.

Hong Kong: Crypto exchange access restricted

Hong Kong's stance on crypto is increasingly at odds with Chinese policy. As China tightens its grip on the region, experts have warned of a potentially spiralling crisis, alongside challenges to growth and innovation.

Among the new rules expected in Hong Kong are:

- Crypto trading will be limited to 'professional investors' with assets over $1m.
- Crypto exchanges will be subject to stringent licensing requirements, similar to those imposed on asset managers dealing with securities.

At the time of writing, only one firm had obtained a license to operate under the current regime, with many firms looking at overseas jurisdictions to set up new businesses.

South Korea: Risk management rules set to come into force

In South Korea, crypto companies face a September 2021 deadline for disclosing their risk management policies and partnerships with banks to ensure that trading accounts are held by real people.

In March, the government issued a revision of the Act on Reporting and Using Specified Financial Transaction Information. This requires crypto exchanges to register with the Korea Financial Intelligence unit (KoFIU) by September 24th. They must meet three core requirements:

- Obtain ISMS certification – this is a security certificate from South Korea's internet security agency. By May, only 20 exchanges had received such certificates.
- Investors must be verified via real-name bank accounts.
- CEOs and board members must be vetted to ensure that they have not committed any crimes.

Policymakers turn their attention to stablecoins

Stablecoins are high on the agenda for the upcoming G20 meeting in Italy on October 30th-31st. In particular, regulators have expressed concern about financial stability. In Europe, fiat-based stablecoins are to be subject to e-money regulations, meaning they will have oversight from central banks.

In the US, the President's Working Group on Financial Markets (PWG) meeting was held in July. The PWG is an inter-agency taskforce that includes leadership from the key financial market regulators and policy makers. Discussion at the July meeting focused on the growth of stablecoins, how they could be used to make payments as well as risks to the financial system and national security.

The US Treasury is also set to issue a report on stablecoins, evaluating their risks and benefits, the current regulatory framework, and providing recommendations for the future. The PWG is keen to move fast on the issue, and is set to release its findings in the next few months.

Wider decentralized finance (DeFi) movement gathers momentum

While DeFi is still at an early stage, its value is growing exponentially. The total value locked into DeFi platforms including collateral pools and smart contracts has soared from less than $1bn in 2019 to $90bn by early June 2021.

DeFi products rely on the use of smart contracts or software protocols/self-executing code that facilitate peer to peer transactions. This has led people to access services including derivatives trading, lending, insurance and asset management without using an intermediary like a bank. It is also driving the creation of new services like margin trading, yield farming, liquidity mining and crypto staking. Yield farming, for example, allows its users to 'hunt for rewards' by interacting with DeFi protocols and temporarily place deposits as collateral into a liquidity pool. This pool can then be used by others, including investors and start-ups, in exchange for financial rewards.

While these new use cases are driving innovation, they are also creating new risks. DeFi hacks totalled $994m in January-August 2021, with the biggest ever hack carried out against Poly Network, totalling $612m. This was the largest crypto-related hack to date, with criminals targeting the smart contract which executes transactions.

Interest in non-fungible tokens (NFTs) has also surged. NFTs are tokens that act as digital representation of ownership of a unique and scarce item such as a piece of art or a collectible item. NFTs have generated $2.5bn so far in 2021, with one representing a piece by digital artist Beeple bought at Christie's, a fine art auction house in London, for $69m. With the art world already synonymous with money laundering, it's possible that NFT trades could ultimately be equated with the purchase and sale of art or antiquities.

Updated FATF guidance on VASPs, to be finalized in November 2021, has been interpreted by some as a step towards the organization capturing certain types of NFTs in the future. In its report FATF stated that it does not "seek to capture the types of closed-loop items that are non-transferable, non-exchangeable, and non-fungible." But it did clarify that the definition of VAs/VASPs is "intended to capture specific financial activities and operations (i.e., transfer, exchange, safekeeping and administration, issuance, etc.) and assets that are convertible or interchangeable—whether virtual-to-virtual, virtual-to-fiat or fiat-to-virtual."

While FATF has indicated it would not change its definition of VASPs, the hacks that have happened this year indicate that regulation around decentralized networks could be needed . In particular, this would place a greater focus on carrying out CDD and KYC checks on customers using exchanges, as well as the development of international standards for smart contracts.

While the future regulation of DeFi remains uncertain, developments in 2021 so far suggest what a new framework could look like. In the US, the Securities and Exchange Commission (SEC) has suggested implementing a 'safe harbor' policy around DeFi – a reference to legal provisions designed to reduce or eliminate legal liabilities under certain circumstances. Disclosure or safe harbor requirements could help regulators better understand how the market is operating, and enable good practice recommendations to be developed.

In August, the SEC settled its first case against a DeFi firm for making false and misleading statements when selling unregistered securities via smart contracts, with a total value of more than $30m.

Exploration of Central Bank Digital Currencies (CBDCs) continues

CBDCs, 'virtual money backed and issued by a central bank', are seen as a way to address financial inclusion. However, concerns about user privacy remain, and there is concern that governments would be able to monitor every transaction an individual makes. Work is therefore ongoing to understand the human rights implications of CBDCs, with safeguards needed to ensure the separation of state and personal finances. The need to carry about CDD checks could also inadvertently lead to the state having a 360-degree financial view on its citizens.

While these debates are ongoing, many countries are continuing to explore the potential of CBDCs. The Atlantic Council's CBDC tracker found that:

- 81 countries are exploring the development of CBDCs.
- 5 CBDCs have been launched, primarily in the Caribbean for retail payments: Bahamas, St Kitts & Nevis, Antigua & Barbuda, Saint Lucia and Grenada.
- A further 14 countries have CBDCs at a pilot stage including UAE, Saudi Arabia, China, Hong Kong, Thailand, Singapore, South Korea, Sweden, Lithuania and Ukraine.

As more countries advance their CBDC programs, the need for international standards and coordination will grow. Serious potential implications for cybersecurity, sanctions evasion and illicit financial flows will need to be addressed. A number of practical questions also remain unanswered: How will digital payments and digital wallets be monitored? Will countries be able to adapt to the use of new technologies?

In authoritarian regimes, CBDCs could also be used to carry out mass surveillance, or to move illicit financial flows linked to proliferation financing, corruption, sanctions evasion, money laundering and terrorist financing.

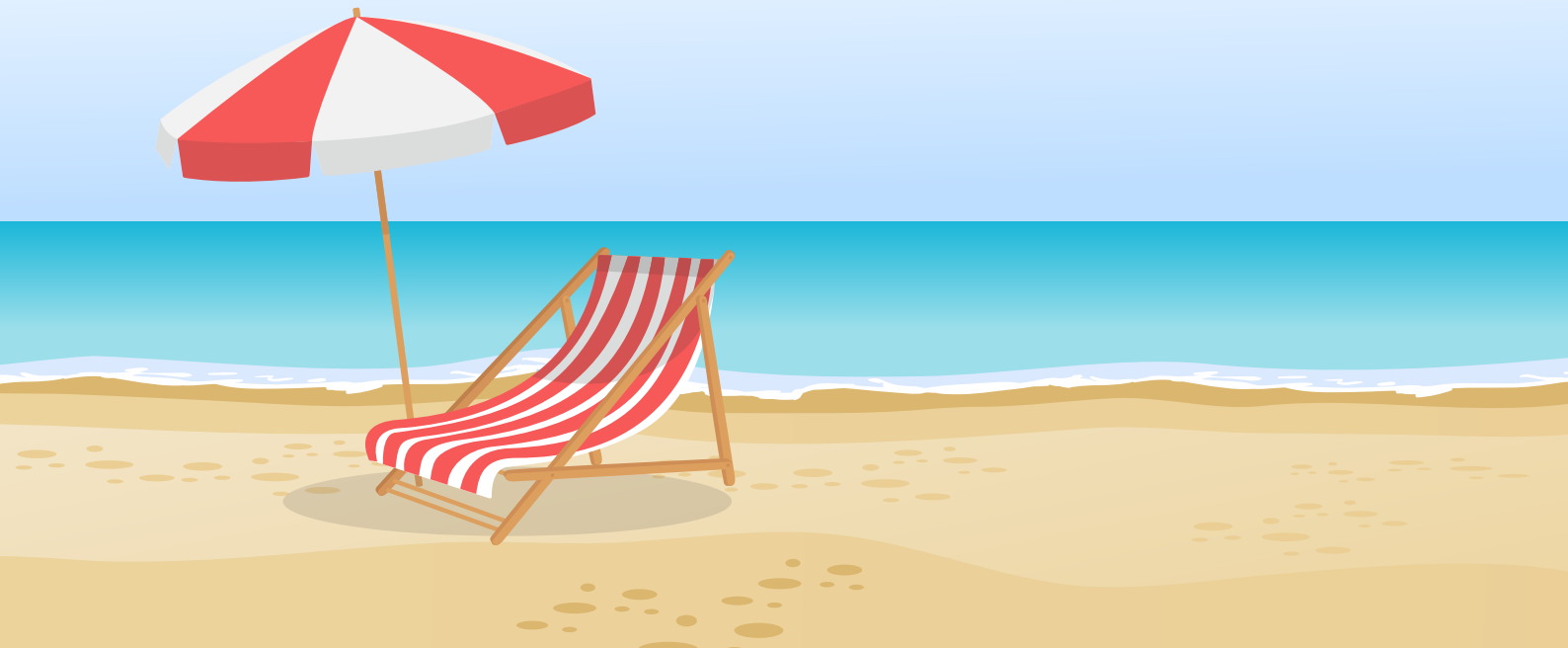
One early potential use case could emerge in China, where the government is aiming to develop an electronic renminbi (the e-CNY) for international travellers to use during the 2022 winter Olympics. Russia also expects to have a digital ruble by late 2021.

What does this mean for my organization?

In addition to AML/CFT registration, crypto firms and VASPs should understand what authorization is needed to operate legally as new legislation is introduced. VASPs, crypto firms and businesses looking to work with them should study FATF's latest guidance, alongside enforcement actions that have been taken. This is required to fully understand the risks, controls and expectations of regulators – including the need to have effective AML/CFT and sanctions programmes in place, as well as geo-blocking as a control.

Firms should update their policies, processes and systems with risk indicators provided by the FATF and guidance issued by local regulators. They should work to engage with FATF's Virtual Assets Contact Group as well as local regulators and policy makers to ensure that their views are considered as regulation is being developed that could affect how their firms operate.

Companies should also look to identify different technology solutions being developed to comply with the travel rule alongside other AML/CFT requirements and engage with different providers to identify compliant solutions. Firms should review data standards that have been developed so they can begin putting the right data capture structures in place to comply with new measures as legislation is introduced. Banks and financial institutions offering services to crypto exchanges and VASPs should ensure that they understand the licensing and authorization regime for their client as well as the control environment of those firms to ensure that downstream risks are adequately managed.



04

What's Next: Dates for your diary: From September to December

Upcoming FATF Mutual Evaluations (Japan, South Africa, Vietnam, Poland, Croatia)

September – Federal elections in Germany

October – FATF Plenary and Working Group meetings

October/November – Hong Kong annual policy address

November 2021 – FATF to issue updated Risk-Based Approach to Virtual Assets

~180 days from June 30th: Update from FinCEN post priorities listing

About ComplyAdvantage

ComplyAdvantage is the financial industry's leading source of AI-driven financial crime risk data and detection technology. ComplyAdvantage's mission is to neutralize the risk of money laundering, terrorist financing, corruption, and other financial crime. More than 800 enterprises in 69 countries rely on ComplyAdvantage to understand the risk of who they're doing business with through the world's only global, real-time database of people and companies. The company actively identifies tens of thousands of risk events from millions of structured and unstructured data points every single day.

ComplyAdvantage has four global hubs located in New York, London, Singapore and Cluj-Napoca and is backed by Goldman Sachs Growth Equity Fund, Ontario Teachers', Index Ventures and Balderton Capital. Learn more at:

complyadvantage.com

Our Customers

Santander GEMINI OakNorth Bank CURVE

raisin. Munich RE Lydia OANDA

Get in Touch

AMER
New York

1460 Broadway
#8000
New York
NY 100136

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

EMEA
London

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

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

APAC
Singapore

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

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

EMEA
Romania

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