Money Laundering Enforcement Trends: Spring 2022

Introduction

Since our previous issue, money laundering enforcement and regulation have been in the spotlight in many regions around the world. Signs point to this trend continuing and we are likely to see money laundering prosecutions employed for specific U.S. policy aims as well, including in the context of efforts against Russia and Belarus in the wake of Russia’s invasion of Ukraine.

Meanwhile, the Financial Crimes Enforcement Network (FinCEN) continues to be an active regulator, most notably regarding the implementation of the Corporate Transparency Act (CTA) and Anti-Money Laundering Act of 2020 (AMLA).

In the enforcement context, U.S. regulators have demonstrated an increased focus on cryptocurrency, not only in their policy positions and public statements but also in the high-profile prosecutions that have been pursued.

Outside the U.S., recent reports from the Financial Action Task Force (FATF) have highlighted changes in the international anti-money laundering (AML) risk landscape, with 10 jurisdictions changing risk classification. In the U.K., increased enforcement has resulted in significant penalties for financial institutions.

In this issue, we highlight the key U.S. regulatory, U.S. enforcement, and international trends of the last few months and briefly
discuss other developments of note.

U.S. Regulatory Developments

U.S. regulators have been very active in their AML efforts. Recently, FinCEN issued an alert addressing increased money laundering concerns in light of the ongoing Russian invasion of Ukraine. FinCEN is also continuing to develop regulations to implement the beneficial ownership registry created through the CTA and is seeking assistance to modernize the BSA as required by the AMLA.

FinCEN Issues Alert on Potential Russian Sanctions Evasion Efforts

On March 7, 2022, FinCEN issued an alert regarding the evasion of sanctions and other measures recently implemented by the U.S. in connection with Russia’s invasion of Ukraine. The alert provides a list of red flags regarding possible sanctions evasion and ransomware attacks, including red flags specific to convertible virtual currency (CVC) transactions.

• CVC-Focused Red Flag Indicators. Several of the red flag indicators focus on CVC transactions. According to the alert:

[w]hile large scale sanctions evasion using CVC by a government such as the Russian Federation is not necessarily practicable, sanctioned persons, illicit actors, and their related networks or facilitators may attempt to use CVC and anonymizing tools to evade U.S. sanctions... CVC exchangers and administrators and other financial institutions may observe attempted or completed transactions tied to CVC wallets or other CVC activity associated with sanctioned Russian, Belarusian, and other affiliated persons.

Red flag indicators related to CVC transactions include: (1) transactions involving IP addresses located in Russia, Belarus, FATF-identified jurisdictions with AML/countering financing of terrorism (CFT)/countering proliferation financing (CPF) deficiencies, sanctioned jurisdictions, or other non-trusted sources; (2) transactions connected to CVC addresses listed on the U.S. Department of the Treasury’s Office of Foreign Assets Control’s (OFAC) Specially Designated Nationals and Blocked Persons List (SDN List); and (3) transactions using a CVC exchanger or foreign-located money services business (MSB) in a high-risk jurisdiction with AML/CFT/CPF deficiencies, including insufficient know-your-customer (KYC) or customer due diligence measures. The focus on CVC transactions in the alert is not surprising given U.S. regulators’ continued focus on virtual currency.

• Updated SAR Filing Instructions. The alert instructs financial institutions to file a suspicious activity report (SAR) on a transaction involving a designated person when also filing a blocking report with OFAC and to notify OFAC of SARs if there is a suspected sanctions connection. Relevant SARs should include the notation: "FIN-2022-RUSSIASANCTIONS."

• Information Sharing Among Financial Institutions Strongly Encouraged. FinCEN "strongly encouraged" financial institutions to share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.

• Use of Innovative Tools to Identify Hidden Assets. Citing a 2018 Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, the alert encourages the “use of innovative tools and solutions” to identify hidden Russian and Belarusian assets. Those “innovative tools” are not described, however.

FinCEN’s Notice of Proposed Rulemaking on Beneficial Ownership Disclosure

FinCEN received more than 237 comments regarding its Notice of Proposed Rulemaking (NPRM) regarding Beneficial
Ownership Reporting Requirements (the Proposed Rule) to implement the CTA before the comment period closed on February 7, 2022. The CTA requires a broad range of qualifying companies, known as “reporting” companies, to provide FinCEN identifying information for all beneficial owners.

The public comments included certain recurring themes that we expect FinCEN to consider as it promulgates its final rule:

- **Cost and Burden**: Many commenters expressed concern about the compliance burden the Proposed Rule will create for small businesses. One commenter stated the Proposed Rule may cause delays in opening bank accounts, as prior registration in the FinCEN portal will be required to open up accounts with financial institutions. Other commenters, however, including the United Brotherhood of Carpenters and Joiners of America (UBC), sought to strengthen and expand the rule “to make the database as useful as possible to law enforcement, intelligence agencies, regulators and financial institutions.”

- **Information Verification Responsibility**: Several commenters suggested working with the Secretary of State for each respective state (with some suggesting a focus on states with high corporate registrations like Delaware) to obtain identifying and beneficial ownership information both at the time of entity formation and when an entity is up for renewal. The Delaware Secretary of State, however, submitted a comment opposing the requirement of states to “remit information utilizing existing processes” as it may result in “inconsistent information” and may impose costly administrative challenges.

- **Data Privacy Considerations**: Another concern of commenters, including the American Bar Association (ABA), is the data privacy implications of a new government database that will hold identifying information on individuals, including social security numbers, after several high-profile data breaches at U.S. government agencies.

- **Deadlines**: A comment signed by members of the real estate industry expressed concern regarding the Proposed Rule’s “shortened deadlines for submission of information.” The Proposed Rule allows 14 days to correct an inaccurately filed report (compared to the current CTA, which provides 90 days) and 30 days to file an updated report or change in exemption status (compared to the current CTA, which requires information be disclosed in a “timely manner and not later than one year”).

FinCEN will consider these comments and issue a final rule regarding the beneficial ownership reporting requirements, likely later this year. FinCEN will also promulgate rules regarding (1) the retention and disclosure of the beneficial ownership data, including how federal, local, and international regulators can obtain access to the information, and (2) updating the customer due diligence rule in light of the beneficial ownership registry. Those rulemaking processes have yet to start.

**BSA Modernization to Protect U.S. National Security and to Keep Pace with Financial Innovations**

On December 14, 2021, FinCEN issued a Request for Information (RFI) seeking comments on ways to streamline, modernize, and update the AML/CFT regime in the United States, as required by Section 6216 of the AMLA. The stated purpose of FinCEN’s review is to ensure proper guidance to safeguard financial systems from financial crime, ensure the continued flow of reporting that has been useful in combatting financial crime, and “identify regulations and guidance that may be outdated redundant, or otherwise do not promote a risk-based AML/CFT compliance regime for financial institutions, or that do not conform with the commitments of the United States to meet international standards to combat money laundering, financing of terrorism, serious tax fraud, or other financial crimes.”

Some of the recurring themes contained in the comments are:

- **Review and Increase of Reporting Thresholds Relating to Currency Transaction Reports (CTRs)**: Some comments sought to increase the current $10,000 reporting requirement, noting that the threshold has not accounted for inflation and current economic realities. The $10,000 threshold was set when the Bank Secrecy Act (BSA) was passed in 1970 and is the equivalent of approximately $74,000 today. Several commentators emphasized that the current threshold creates disproportionate costs and diverts resources away from high-risk transactions.
**Cryptocurrencies.** Some comments urged FinCEN to provide guidance on how cryptocurrencies can demonstrate compliance with AML regulations. For example, a financial institution commenter highlighted the need for “expanded guidance on expected responsibilities of financial institution(s) with respect to monitoring and reporting suspicious activity” associated with virtual currencies. Another commenter suggested that cryptocurrency transactions be “clearly identified in some manner within payment systems by code or common description properties.”

**Assess FBAR Reporting Requirements.** In addition, several comments sought greater clarity regarding the reporting requirements related to Foreign Bank and Financial Accounts Reports (FBARs), which impose reporting requirements to U.S. citizens who have a financial interest over foreign financial accounts exceeding $10,000. Comments emphasized that the current reporting threshold unfairly targets U.S. citizens living abroad and is not appropriately tailored to high-risk transactions. Moreover, many comments urged FinCEN to move to a residence-based taxation scheme.

**Other Notable U.S. Regulatory Developments**

There have been a number of other notable AML-related regulatory developments in the past six months, including:

- **All-Cash Real Estate Transactions.** On December 6, 2021, FinCEN published an Advance Notice of Proposed Rulemaking (ANPRM) to solicit public comment on a potential rule that would impose nationwide recordkeeping and reporting obligations on certain parties participating in all-cash real estate transactions. According to FinCEN, “when real estate is purchased without... financing, it can be nearly impossible to trace the beneficial owners behind shell companies ...” This priority is highlighted in the Biden administration’s Strategy on Countering Corruption (SCC). The comment period closed February 7, 2022, and FinCEN will next issue an NPRM.

- **ENABLERS Act.** The Establishing New Authorities for Business Laundering and Enabling Risks to Security Act (ENABLERS Act) was introduced in the U.S. House of Representatives by Representative Tom Malinowski (D-NJ) on October 8, 2021. The legislation would make “gatekeeper professions” (i.e., accountants, lawyers, art dealers, trust service providers, public relations businesses, and investment advisors) covered by the BSA’s definition of “financial institutions.”

- **Proposals to Expand AML Regulations to Cover the Private Investment Industry.** The SCC specifies that the Treasury Department will revisit a 2015 NPRM that sought to impose AML requirements for investment advisers such as hedge funds and private equity funds. Specifically, the 2015 NPRM proposed to define an “investment adviser” as “[a]ny person who is registered or required to register with the SEC under section 203 of the Investment Advisers Act of 1940 (15 U.S.C. 80b-3(a)).” The SCC also instructs the Treasury Department to consider whether to extend the existing AML regime to private placement funds, including investment offered by hedge funds and private equity funds.

**U.S. Enforcement Developments**

U.S. money laundering enforcement was not particularly active over the past few months, but there has been a clear trend spanning U.S. enforcement agencies to increase enforcement against those who misuse cryptocurrency.

**Increased Focus on Cryptocurrency**

Cryptocurrencies continue to grow in popularity and create risk that they will be used in illicit financial transactions. One recent report found that cryptocurrency-based crime nearly doubled in 2021 with illicit addresses receiving $14 billion in assets, up from $7.8 billion in 2020. In March, President Biden signed an executive order highlighting a “whole-of-government approach to addressing the risks and harnessing the potential benefits of digital assets and their underlying technology.” The U.S. Department of Justice (DOJ), FinCEN, and OFAC have all taken similar steps to address the threats posed by cryptocurrency and recent actions back up the policies statements, all of which strongly suggests an increased focus on cryptocurrency enforcement in 2022.

- The DOJ continues its focus on high-risk cryptocurrency businesses. Building upon the publication of its Cryptocurrency Enforcement Framework, in October 2021, the DOJ announced the creation of a National Cryptocurrency Enforcement Team.
(NCET) dedicated to investigating and prosecuting cryptocurrency cases. NCET will focus its efforts on “criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors.” These types of high-risk business models were the focus of the Cryptocurrency Enforcement Framework (discussed in Winter 2021) and have traditionally been the focus of U.S. regulators. The Biden administration also highlighted the role of cryptocurrency in corruption in the SCC, which noted the creation of the NCET as part of its strategy to “Hold[] Corrupt Actors Accountable” and said it would focus “particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors.”

A recent prosecution by the DOJ shows this focus on mixers which provide anonymity and suggest additional cases to come in 2022. On August 18, 2021, Larry Dean Harmon pleaded guilty to one charge of money laundering conspiracy in connection with his operation of Helix, a bitcoin mixer based on the darknet and operated as a cryptocurrency laundering service. Mixers such as Helix offer increased anonymity to customers by combining various streams of cryptocurrency funds. As a result, Helix, which Harmon operated from 2014 to 2017, allowed customers to send bitcoin to others while concealing the source of the bitcoin. Helix ultimately facilitated the transfer of over 350,000 bitcoin with a value of over $300 million. Beyond his operation of the mixer, Harmon also promoted Helix as having the capability to hide transactions from law enforcement. Through Helix, Harmon helped launder money from criminal activities, such as drug trafficking, and concealed that money from the government. Harmon’s guilty plea included a guideline sentence of life in prison, which suggests Harmon is hoping for a below-guidelines sentence based on substantial cooperation. In November 2021, the government confirmed that Harmon was working as a cooperator, writing in a status report to the court that “Defendant’s cooperation remains active and ongoing” and seeking to defer his sentencing until the cooperation is complete.

Though the DOJ has expressed a focus on infrastructure actors, we have also seen recent prosecutions for traditional money laundering using cryptocurrency. On January 18, 2022, Robert O’Neill pleaded guilty to charges relating to distributing marijuana and laundering the cryptocurrency proceeds through a darknet vendor known as GOLD. Records indicate that O’Neill sold marijuana in exchange for bitcoin and after receiving payment, provided the bitcoin to GOLD in exchange for cash. From September 2015 to May 2018, O’Neill laundered more than $725,000 through GOLD and another $167,000 through another co-conspirator.

On February 8, 2022, the DOJ announced the arrests of and charges against two individuals who allegedly laundered bitcoin stolen in the 2016 hack of virtual currency exchange Bitfinex. The press release announcing the hack said that law enforcement had seized more than $3.6 billion in cryptocurrency related to the Bitfinex hack as of February 2022.

• FinCEN’s biggest monetary penalty of 2021 was against a convertible virtual currency exchange. On August 10, 2021, FinCEN announced that it assessed a civil monetary penalty of $100 million against BitMEX, a convertible virtual currency derivatives exchange that offers futures, options, and swaps in cryptocurrencies. FinCEN found that between 2014 and 2020, BitMEX violated the BSA by failing to implement an adequate anti-money laundering program, verify customers’ identities, and file SARs in at least 588 transactions. As FinCEN explained, “BitMEX conducted at least $209 million worth of transactions with known darknet markets or unregistered money services businesses providing mixing services,” and some transactions involved “high-risk jurisdictions and alleged fraud schemes.” BitMEX also failed to implement adequate controls to ensure it did not conduct business with persons located in the U.S and in some cases, even altered customers’ location information. Under the settlement with FinCEN, not only will BitMEX pay the $100 million civil penalty, but independent consultants will also analyze BitMEX’s historical transaction data and ensure effective policies, procedures, and controls are implemented to prevent BitMEX from operating in the U.S. BitMEX also settled with the Commodity Futures Trading Commission (CFTC) as part of a global settlement related to this conduct.

The $100 million penalty matched with FinCEN imposed on Capital One in January 2021 as the highest penalty of 2021. It is clear that FinCEN intends to send a message that it will vigorously enforce the BSA AML requirements, even against institutions dealing with digital assets. In a speech to the American Bankers Association/American Bar Association Financial Crimes Enforcement Conference in January 2022, Acting Director of FinCEN Him Das made this point explicitly, saying: “By assessing
Other Key U.S. Enforcement Actions

In addition to broad focus on cryptocurrency enforcement, U.S. enforcement agencies have continued to investigate and resolve traditional money laundering offenses. A few enforcement actions are particularly noteworthy:

- **Credit Suisse agreed to DPA and nearly $550 million in global penalties.** In October 2021, Switzerland-based global financial institution Credit Suisse Group AG and its U.K. subsidiary Credit Suisse Securities (Europe) Limited (CSSEL) (together, Credit Suisse) admitted to using the U.S. financial system to defraud U.S. and international investors between 2013 and 2017 in the financing of an $850 million loan for a tuna fishing project in Mozambique. Credit Suisse Group AG entered into a three-year deferred prosecution agreement (DPA) with the DOJ in connection with a charge of conspiracy to commit wire fraud and CSSEL pleaded guilty to a conspiracy to commit wire fraud. Credit Suisse has been assessed more than $547 million in penalties, fines, and disgorgement in the U.S. and U.K., approximately $175.5 million of which it must pay to the U.S. According to a DOJ press release, “the total penalty reflects a 15% reduction off the bottom of the applicable U.S. Sentencing Guidelines range.” The DOJ considered several factors in reaching this resolution with Credit Suisse, including its failure to voluntarily disclose, the nature and seriousness of the offense, and significant delays in producing relevant evidence. However, Credit Suisse has agreed to cooperate with the DOJ, enhance its compliance program and internal controls, and submit yearly reports to the DOJ to ensure that its compliance program is effective in deterring money laundering violations, among others.

- **Community Bank of Texas penalized for BSA violations.** On December 16, 2021, FinCEN announced that Community Bank of Texas (CBOT), a wholly owned subsidiary of CBTX, Inc. (a bank holding company that operates 35 branches in Texas) has incurred $8 million in civil penalties — $7 million from FinCEN and $1 million from the Office of the Comptroller of the Currency (OCC) — for BSA violations. During at least 2015 through 2019, CBOT admitted to failing to implement and maintain an effective AML program and failing to report hundreds of suspicious transactions to FinCEN even after CBOT became aware that certain customers were subjects of criminal investigations. As a result, CBOT caused millions of dollars in suspicious transactions to go unreported to FinCEN, including transactions connected to money laundering.

- **U.S. district court indicted former senior Venezuelan prosecutors on money laundering charges for receiving over $1 million in bribes.** In an example of money laundering prosecutions as a tool to target bribe recipients, on March, 8 2022, two former senior Venezuelan prosecutors, Daniel D’Andrea Golindano (D’Andrea), and Luis Javier Sanchez Rangel (Sanchez), were indicted in the U.S District Court for the Southern District of Florida on charges of conspiracy to commit money laundering and as well as engaging in monetary transactions involving criminally derived property. The indictment alleges that in or around 2017, D’Andrea and Sanchez, in their capacity as prosecutors of the anti-corruption unit of the Venezuelan Attorney General’s Office, discussed, agreed, and received bribes of more than one million dollars in exchange for dropping criminal charges against an identified recipient.

- **OFAC has identified cryptocurrency as a threat to the effectiveness of its sanctions regime.** The Treasury 2021 Sanctions Review, published in October 2021, focused on the role that cryptocurrency plays in sanctions enforcement, noting that “if left unchecked, these digital assets and payments systems could harm the efficacy of our sanctions.” A couple recent resolutions with companies operating cryptocurrency services for failing to implement adequate controls to prevent individuals located in sanctioned jurisdictions from utilizing their services showcase the role that OFAC will play in cryptocurrency enforcement. In December 2020, BitGo, Inc. agreed to pay $98,830 to resolve civil liability for allowing individuals located in the sanctioned jurisdictions of Crimea, Cuba, Iran, Sudan, and Syria to use BitGo’s digital wallet management service to trade in digital currencies. Similarly, in February 2021, BitPay, Inc., a bitcoin payment service provider that allows merchants to accept payments in digital currency, agreed to pay $507,375 after receiving digital currency from individuals located in various sanctioned jurisdictions and converting it for merchants. And in March 2021, Coinbase Global, Inc., a cryptocurrency exchange, also announced that certain of its voluntary disclosures were “under review by OFAC,” and those transactions were still under review as Coinbase’s latest 10-Q in November 2021. It is likely that investigations into the use of cryptocurrency to avoid sanctions will be an area of focus for OFAC in 2022.

In an example of money laundering prosecutions as a tool to target bribe recipients, on March, 8 2022, two former senior Venezuelan prosecutors, Daniel D’Andrea Golindano (D’Andrea), and Luis Javier Sanchez Rangel (Sanchez), were indicted in the U.S. district court for the Southern District of Florida on charges of conspiracy to commit money laundering and as well as engaging in monetary transactions involving criminally derived property. The indictment alleges that in or around 2017, D’Andrea and Sanchez, in their capacity as prosecutors of the anti-corruption unit of the Venezuelan Attorney General’s Office, discussed, agreed, and received bribes of more than one million dollars in exchange for dropping criminal charges against an identified recipient.

In an example of money laundering prosecutions as a tool to target bribe recipients, on March, 8 2022, two former senior Venezuelan prosecutors, Daniel D’Andrea Golindano (D’Andrea), and Luis Javier Sanchez Rangel (Sanchez), were indicted in the U.S. district court for the Southern District of Florida on charges of conspiracy to commit money laundering and as well as engaging in monetary transactions involving criminally derived property. The indictment alleges that in or around 2017, D’Andrea and Sanchez, in their capacity as prosecutors of the anti-corruption unit of the Venezuelan Attorney General’s Office, discussed, agreed, and received bribes of more than one million dollars in exchange for dropping criminal charges against an identified recipient.

In an example of money laundering prosecutions as a tool to target bribe recipients, on March, 8 2022, two former senior Venezuelan prosecutors, Daniel D’Andrea Golindano (D’Andrea), and Luis Javier Sanchez Rangel (Sanchez), were indicted in the U.S. district court for the Southern District of Florida on charges of conspiracy to commit money laundering and as well as engaging in monetary transactions involving criminally derived property. The indictment alleges that in or around 2017, D’Andrea and Sanchez, in their capacity as prosecutors of the anti-corruption unit of the Venezuelan Attorney General’s Office, discussed, agreed, and received bribes of more than one million dollars in exchange for dropping criminal charges against an identified recipient.

In an example of money laundering prosecutions as a tool to target bribe recipients, on March, 8 2022, two former senior Venezuelan prosecutors, Daniel D’Andrea Golindano (D’Andrea), and Luis Javier Sanchez Rangel (Sanchez), were indicted in the U.S. district court for the Southern District of Florida on charges of conspiracy to commit money laundering and as well as engaging in monetary transactions involving criminally derived property. The indictment alleges that in or around 2017, D’Andrea and Sanchez, in their capacity as prosecutors of the anti-corruption unit of the Venezuelan Attorney General’s Office, discussed, agreed, and received bribes of more than one million dollars in exchange for dropping criminal charges against an identified recipient.
contractor and others who were the subject of a government investigation on alleged corruption involving contracts with subsidiaries of Venezuela’s state-owned oil company, Petróleos de Venezuela, S.A. (PDVSA). According to the indictment, D’Andrea arranged for a co-conspirator to create false invoices seeking payment for over $1 million dollars in equipment from a contractor, who in turn paid the sums to an account in the Southern District of Florida for the benefit of D’Andrea and Sanchez. D’Andrea and Sanchez allegedly caused the Venezuelan Attorney General’s Office not to pursue criminal charges against the contractor and other conspirators.

- **Sons of Panamanian president pled guilty to money laundering stemming from Odebrecht bribery scheme**. In December, 2021, Ricardo Alberto Martinelli Linares, 42, and Luis Enrique Martinelli Linares, 39, sons of the former Panamanian President Ricardo Martinelli, pleaded guilty to laundering $28 million in connection with the massive bribery scheme involving Brazilian global construction conglomerate Odebrecht. The guilty pleas are the latest of a number of follow-on charges to the bribery scheme that resulted in Odebrecht and Braskem agreeing to pay at least $3.5 billion in combined global penalties in settlement with U.S., Swiss, and Brazilian authorities. The SCC put significant focus on attacking the demand side of bribery and these prosecutions for money laundering is illustrative of how DOJ could target the demand side of bribery when it cannot bring other charges. The Martinelli brothers admittedly conspired with each other and others to establish offshore bank accounts in the names of shell companies to receive and disguise bribe proceeds from Odebrecht. The brothers wired funds in and out of the U.S., where they purchased a yacht and a condominium. After entering their guilty pleas, they agreed to a forfeiture amount of approximately $18.9 million. They are scheduled to be sentenced in May 2022.

**International Developments**

International efforts to combat money laundering have also been notable in the past few months. FATF issued changes in risk classifications for 12 jurisdictions, U.K. authorities have noticeably increased enforcement, and cryptocurrency markets have been the focus of international regulators as well.

**Notable Developments in AML Risk Classifications**

Recent reports from the FATF have highlighted changes in the international AML risk landscape. The FATF classifies countries according to AML and CFT risks, maintaining both a list of high-risk jurisdictions subject to a Call for Action (also known as the “black list”) – which identifies jurisdictions which the FATF has called upon to apply significant measures to prevent money laundering, terrorist financing, and proliferation financing – and jurisdictions under Increased Monitoring (also known as the “grey list”), which identifies countries with "strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing" but which have committed to resolve the deficiencies “swiftly.” In February 2020, the FATF paused its review of countries on the black list (only Iran and North Korea), but has since continued to review countries on the grey list. In 2021, the FATF removed three countries and added seven countries to the grey list. So far in 2022, the FATF has added one country and removed one country from the grey list.
### Added to Grey List

<table>
<thead>
<tr>
<th>Country</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Haiti</td>
<td>June 2021</td>
</tr>
<tr>
<td>Malta</td>
<td>June 2021</td>
</tr>
<tr>
<td>Philippines</td>
<td>June 2021</td>
</tr>
<tr>
<td>South Sudan</td>
<td>June 2021</td>
</tr>
<tr>
<td>Jordan</td>
<td>October 2021</td>
</tr>
<tr>
<td>Mali</td>
<td>October 2021</td>
</tr>
<tr>
<td>Turkey</td>
<td>October 2021</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>March 2022</td>
</tr>
</tbody>
</table>

### Removed from Grey List

<table>
<thead>
<tr>
<th>Country</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ghana</td>
<td>June 2021</td>
</tr>
<tr>
<td>Mauritius</td>
<td>October 2021</td>
</tr>
<tr>
<td>Botswana</td>
<td>October 2021</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>March 2022</td>
</tr>
</tbody>
</table>

Other notable developments regarding changes to risk classification include:

- In a June 2021 joint report by the FATF and the Asia-Pacific Group on Money Laundering, the groups stated that Japanese law enforcement “needs to focus more on the laundering of proceeds in complex large-scale cases often involving fraud and drug-related crimes.” Specifically, the report found that the country faces risks related to the activities of criminal gangs, known as Bōryokudan, including drug trafficking, illegal remittances, and money extortion.

- In January 2022, the European Union (EU) removed the Bahamas from its own AML black list (which, while taking into account FATF classifications, is maintained separately and subjects financial institutions to heightened scrutiny from EU regulators). According to EU Attorney General Ryan Pinder, the Bahamas addressed systemic deficiencies in its AML and CTF mechanisms and “engaged in diplomatic and technical meetings on an ongoing basis” to get itself removed from the black list. One of the measures the Bahamas took leading to delisting was the introduction of a bill to require beneficial ownership information for segregated accounts companies (SACs) and non-profit organizations limited by shares under the scope of the Register of Beneficial Ownership Act’s scope, to be accessible to the Attorney General. The Bahamas was previously removed from the FATF grey list in December 2020.

### Significant Increase in U.K. AML Enforcement Activity

The U.K. government has increasingly demonstrated its commitment to investigating and prosecuting serious financial misconduct and has levied historic fines against financial services institutions that fall afoul of the country's AML regulations at all levels.

Record fines against financial institutions such as NatWest and HSBC have all contributed to a climate of increasing AML enforcement actions. This festival of enforcement in the U.K. extends beyond Financial Conduct Authority (FCA)-led actions and include actions by other regulatory bodies such as the Solicitors Regulation Authority (SRA), which has fined one of the U.K.’s most prestigious law firms the record amount of £232,500 (approximately $315,000) for failing to carry out the required level of due diligence or ongoing monitoring.

In the coming months we can anticipate more decisions in AML enforcement actions as the FCA has over 40 active cases where regulators are investigating financial services providers for breach of AML and due diligence requirements. It is also worth noting that despite the recent success of the FCA in its criminal case against National Westminster Bank Plc (NatWest), only two of the known 40 active FCA cases are criminal, indicating that despite the FCA’s signaling of the increased use of its criminal prosecutorial power, the risk that companies in the U.K. will face criminal prosecution in AML actions remains low.
• **NatWest fined $350 million for AML failures in first successful criminal prosecution under the U.K.’s Money Laundering Regulations (MLR).** In December 2021, NatWest was fined £264,772,619.95 (approximately $350 million) after the U.K.-based financial services provider was convicted of three offences of failing to comply with money laundering regulations. This judgment is the culmination of a criminal action against NatWest initiated by the FCA in March 2021. The charges against NatWest cover a range of failures including NatWest’s failure to investigate and take action on money laundering “red flags” surrounding the activity of a commercial customer, who deposited approximately £365 million with the bank, of which around £264 million was in cash. This conviction and fine marks the first successful criminal prosecution under the MLR 2007 by the FCA and the first prosecution under the MLR against a bank.

• **FCA fined HSBC $85 Million for lax AML controls.** In December 2021, the FCA fined HSBC Bank plc (HSBC) a discounted amount of £63,946,800 (approximately $80 million) for several AML failures between 2010 and 2018, including a failure to improve its internal controls and risk assessment processes. Specifically, the FCA faulted HSBC, which uses automated processes to monitor transactions, for not: (1) considering whether scenarios used to identify indicators of money laundering of terrorist financing were adequate until 2014 and not conducting risk assessments for new scenarios until 2016; (2) appropriately testing and updating the system parameters used to flag suspicious activity; and (3) checking the accuracy and completeness of data in the monitoring systems. HSBC did not dispute the FCA’s findings. HSBC received a 30 percent discount for agreeing “to settle at the earliest possible opportunity.” HSBC also agreed to implement FCA-supervised remediation of its AML processes.

• **Risks in U.K.’s e-payment sector.** According to a December 2021 Transparency International U.K. report, 38 percent of the country’s e-payment firms had “potential money laundering red flags.” The report indicated risks of money laundering, rather than actual wrongdoing; the risks included “being named as having poor anti-money laundering controls or processing criminal wealth; having owners, directors, or senior members of staff named in money laundering investigations; or owners, directors, or senior members of staff having worked previously for institutions alleged or proven to have anti-money laundering failings.” The risks come at a time of prominence of e-firms in the country, as the e-payment sector made more $660.2 billion worth of transactions in 2020 and 2021. The report examined all 261 firms in the country that had been granted permission by the FCA to operate as an Electronic Money Institution (EMI).

**International Focus on Cryptocurrency Enforcement**

There has been significant tightening of anti-money laundering regulations in markets that offer cryptocurrency through the last quarter of 2021 and into 2022. For example:

• **Turkish government fines Binance Turkey for violating AML regulations.** In December 2021, the Financial Crimes Investigation Board of Turkey (Masak) announced a $750,000 fine against Binance Turkey for violating the AML regulations in Turkey. This fine, which is the maximum fine under Turkey’s Law 5549 on the Prevention of Laundering Proceeds of Crime, marks the first time a cryptocurrency firm has been found guilty of an AML violation under the new law.

• **South Korea’s FIU to conduct AML inspections.** In January 2022, the Financial Intelligence Unit of South Korea’s Financial Services Commission (FIU) announced that it will for the first time carry out inspections of 124 electronic financial service providers to ensure compliance with due diligence requirements, internal control systems and suspicious transaction reporting systems. This inspection is the first of its kind on cryptocurrency providers after Korea’s March 2021 introduction of a revised rule mandating AML compliance on virtual asset service providers. Companies that are found to have breached money laundering regulations may be penalized with full or partial business suspension of up to six months, while individuals may receive a jail term of up to five years or penalty of up to approximately 100 million won (approximately $83,829).
The Money Laundering Regulations 2007 (MLR 2007) have been superseded by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) for conduct that takes place after June 2017. The proceedings against NatWest were brought under MLR 2007 (MLR 2007 and MLR 2017 are referred to together as MLR).

The information contained in this communication is not intended as legal advice or as an opinion on specific facts. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. For more information, please contact one of the senders or your existing Miller & Chevalier lawyer contact. The invitation to contact the firm and its lawyers is not to be construed as a solicitation for legal work. Any new lawyer-client relationship will be confirmed in writing.

This, and related communications, are protected by copyright laws and treaties. You may make a single copy for personal use. You may make copies for others, but not for commercial purposes. If you give a copy to anyone else, it must be in its original, unmodified form, and must include all attributions of authorship, copyright notices, and republication notices. Except as described above, it is unlawful to copy, republish, redistribute, and/or alter this presentation without prior written consent of the copyright holder.