

Money Laundering Enforcement Trends: Fall 2019

White Collar Alert

11.12.2019

FEATURED IN THIS EDITION

Introduction

Increase in Enforcement Resources

Regulatory Updates

- U.S.
- Europe

Emphasis on AML Compliance Programs

Continued Sanctions Enforcement

Actions Against Individuals

Cryptocurrency

Update on International Money Laundering Scandals

- Danske Bank Scandal
- Investigation of Swedbank

Spotlight on Brazil

Introduction

U.S. authorities are committing additional resources to combat money laundering: the FBI announced this year that it would devote additional resources to combatting money laundering and the Financial Crimes Enforcement Network (FinCEN) launched its [Global Investigations Division](#) (GID), which is tasked with carrying out "targeted investigation strategies" to "combat illicit finance threats and related crimes, both domestically and internationally." We continue to see a corresponding growing recognition of the importance of anti-money laundering (AML) compliance programs among companies and enforcement authorities. Notably, *Global Investigations Review* recently [reported](#) that the Securities and Exchange Commission (SEC) may be advancing a theory of money laundering liability in the context of its U.S. Foreign Corrupt Practices Act enforcement of books and records and internal controls provisions. This may add to the pressure on companies to ensure AML and Bank Secrecy Act (BSA) compliance programs are up to date.

It is worth noting that the effects of criminal prosecutions and enforcement actions have been recognized recently not only by their direct targets: credit rating agency FitchRatings recently [stated](#) that AML controls are playing a bigger role in credit ratings because authorities are taking more action against financial institutions with weak controls.

This fall, we follow up on some themes in money laundering enforcement: the government's continued focus on the importance of

BSA/AML [compliance programs](#); significant criminal cases involving [economic sanctions violations](#); and the regulation of [cryptocurrencies](#), which are considered to be high risk for money laundering. We also highlight key U.S. and foreign AML regulatory developments, as well as an important ruling from the [Ninth Circuit](#) and provide an update on two of the high-profile international money laundering scandals currently making headlines: [Danske Bank](#) and [Swedbank](#).

For our country close-up [Spotlight](#) section, we focus on Brazil, where a recent Supreme Court decision may make it more difficult for authorities to investigate potential money laundering.

Increase in Enforcement Resources

In the last six months, the U.S. government has demonstrated an increased focus on money laundering by creating a new unit at FinCEN and a new FBI field office in Miami.

- **New FinCEN Division Focuses on Identifying Primary Foreign Money Laundering Threats.** On August 28, 2019, FinCEN [announced](#) the launch of a new Global Investigations Division (GID), whose mandate includes carrying out "targeted investigation strategies rooted in FinCEN's unique authorities under the Bank Secrecy Act (BSA) to combat illicit finance threats and related crimes, both domestically and internationally." The new division will reportedly leverage FinCEN's powers under Section 311 of the USA Patriot Act and increase collaboration with corresponding foreign entities to focus on potential money laundering and terrorist financing activities. FinCEN's press release explains, "FinCEN's strategic use of its Section 311 authority as well as its other information collection authorities, such as the geographic targeting order and foreign financial agency regulation authorities, have greatly expanded in recent years," and the new GID will enable FinCEN to effectively exercise its authority.
- **New FBI Squad in Miami.** Continuing a trend we highlighted [previously](#), the U.S. government is taking steps to strengthen its ability to target corruption through pursuit of money laundering violations. In March 2019, the FBI [announced](#) that due to the success of its international corruption squads in New York, Los Angeles, and Washington D.C., it would open a field office in Miami. Like other FBI international corruption squads, the newly formed task force is focusing on international bribery, kleptocracy, money laundering, and international antitrust matters.

Why Miami? As we noted in [Spring 2019](#), FinCEN last year issued a [Geographic Targeting Order](#) that requires the collection and reporting by U.S. title insurance companies of certain information involved in residential real estate transactions. [News reports](#) have included speculation that an uptick in such reporting in Miami contributed to the FBI's desire to open a squad office in the area.

Regulatory Updates

U.S.

Meanwhile, banking regulators have also increased their focus on money laundering concerns. On July 22, 2019 the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency (OCC) and FinCEN issued the [Joint Statement on Risk – Focused Bank Secrecy Act/Anti-Money Laundering Supervision](#). The Joint Statement underscores the agencies' expectation that banks will engage in risk assessments and calibrate their BSA/AML programs to identified risks. Notably, the Joint Statement does not encourage banks to de-risk by ceasing to provide certain services or operate in certain jurisdictions that may be considered high risk.

According to the Joint Statement, in regulatory agencies' examinations of banks, "[e]xaminers review risk management practices to evaluate and assess whether a bank has developed and implemented effective processes to identify, measure, monitor, and control risks." Such examinations are tailored by the regulating agencies in order to assess the particular profile risk of the bank. The Joint Statement lists the following common practices for assessing banks' risk profiles, which banks should consider in their own processes:

- leveraging available information, including the bank's BSA/AML risk assessment, independent testing or audits, analyses, and conclusions from previous examinations, and other information available through the off-site monitoring process or a request letter to the bank;
- contacting banks between examinations or prior to finalizing the scope of an examination; and
- considering the bank's ability to identify, measure, monitor, and controls risks.

Europe

EU Member States have until January 2020 to Implement the Provisions of the EU Fifth AML Directive. EU member states will have until January 10, 2020 to implement in their national legislation the provisions of the [EU Fifth AML Directive](#) (5AMLD), some of which impose potentially onerous new requirements. On April 19, 2018 and May 14, 2018, the [European Parliament](#) and the [European Council](#) adopted the 5AMLD. 5AMLD came into force on July 9, 2018 and represents the latest update to the EU's AML directives. It modified the EU Fourth AML Directive (4AMLD) and was part of EU's action plan against terrorism and towards increased transparency, partly as a reaction to the wave of terrorist attacks in Paris and Brussels in November 2015 and March 2016, which "have brought to light emerging new trends, in particular regarding the way terrorist groups finance and conduct their operations," and to the Panama Papers scandal in April 2016. According to rating agency [FitchRatings](#), the EU's push for implementation of 5AMLD "should ultimately be credit positive for banks."

According to the European Commission, 5AMLD's [amendments](#) to 4AMLD "introduce substantial improvements to better equip the EU to prevent the financial system from being used for money laundering and for funding terrorist activities." 5AMLD makes key changes in the following several broad thematic areas as summarized below: 1) the scope of the regulation; 2) access to information on beneficial ownership; 3) creation of centralized national registers; and 4) enhanced due diligence criteria for high-risk countries. Specifically, [5AMLD](#):

- Extends AML and counter-terrorism financing rules to virtual currencies, all forms of tax advisory services, estate agents, and art dealers. These "obliged entities" will now have to conduct due diligence and ongoing monitoring and reporting of suspicious transactions just like financial institutions;
- Enhances access to and transparency of beneficial ownership information by establishing publicly available registers for companies, trusts, and other legal arrangements;
- Enhances the powers of the EU Financial Intelligence Units (FIUs) and facilitates their cooperation by introducing centralized bank and payment account registers, aligning the rules with the latest international standards, and providing them with access to broad information for the carrying out of their tasks;
- Limits anonymity related to virtual currencies, wallet providers, and prepaid cards, including by bringing virtual currency platforms and wallet providers within the definition of "obliged entities" thereby requiring them, among other things, to register with national AML authorities and identify and report suspicious activities;
- Broadens the criteria for the assessment of high-risk countries and improves the checks on financial transactions involving such countries, by requiring member states to, among other things, 1) apply a minimum set of enhanced due diligence requirements that obliged entities will have to apply; and 2) publish and submit to the European Commission periodic risk assessment reports containing data on the volume of supervision and enforcement activity undertaken and amounts of resources spent to meet the objectives of 5AMLD. 5AMLD also establishes centralized national registers of bank and payment account information in all EU member states, and enhances the cooperation among financial supervisory authorities.

5AMLD demonstrates the EU's increased efforts to combat money laundering and terrorist financing. It also reflects the global trend towards tightening the requirements of AML and KYC regulations. Also noteworthy is the fact that 5AMLD is a "minimum harmonisation directive," thus giving the EU member states the option to apply even more stringent requirements at their national

levels.

Emphasis on AML Compliance Programs

U.S. enforcement agencies continue to take action against financial institutions for AML compliance program failures, including inattention to red flags and failure to file Suspicious Activity Reports (SARs).

- **Cease-and-Desist Order against Wilson-Davis & Co. (Wilson), for failing to file SARs during 2013-2017.** Specifically, according to the May 15, 2019 Order, Wilson, a broker-dealer, "ignored numerous red flags listed in its AML policies, failed to properly investigate certain conduct, and ultimately failed to file SARs on the suspicious activity," according to the Order. The Order notes that Wilson's customers exhibited red flags, such as "depositing a physical certificate, liquidating shortly after the deposit, and wiring the proceeds." The SEC drew attention to the fact that Wilson noted existing red flags, and responded by freezing and closing customer accounts, as well as informing a customer that it should seek a new attorney who was at an "arm's length away from the company" to write opinions regarding an issuer, but, despite these actions, did not file the required SARs. As a result, the SEC censured Wilson and Wilson was required to pay a civil money penalty of 300,000 dollars and retain an Independent AML Consultant.
- **Gelband & Co., Inc. (Gelband) issued a Letter of Acceptance, Waiver and Consent to FINRA in connection with allegations that it had failed to conduct independent testing of its AML compliance program during 2014-2017.** According to Gelband's April 2019 Letter, Gelband, a placement agent, "had its designated AML Compliance Officer, or someone who reported to him, conduct the annual testing of its AML program," in violation of FINRA Rule 3310, rendering the testing not "independent." Gelband agreed to pay FINRA a fine of 5,000 dollars.

In addition, a recent case highlights disputes on the oversight of financial institutions. In June 2019, Mitsubishi UFJ Ginko (MUFG), Japan's largest bank (formerly The Bank of Tokyo-Mitsubishi UJF, Ltd.), agreed to pay 33 million dollars to the New York Department of Financial Services (NYDFS) to settle a federal civil litigation in the Southern District of New York, which arose because of a dispute between the parties concerning NYDFS' oversight. MUFG had sought to convert oversight of its branches from NY to OCC. (See [OCC Conditional Approval](#)). In November 2017, the OCC granted conditional approval for the change, noting that MUFG's New York branches were still subject to two consent orders issued by NYDFS, which flagged potential deficiencies in its programs, policies, and procedures regarding BSA/AML compliance, as well as compliance with regulations of the Office of Foreign Assets Control (OFAC).

Litigation between NYDFS and MUFG [ensued](#). NYDFS argued that MUFG had used branch conversion to evade New York's investigation. As part of its recent settlement agreement with MUFG, NYDFS has promised not to challenge the OCC license and to release MUFG from liability with regards to any claims alleging that MUFG violated New York banking law before OCC approved MUFG's federal license.

Continued Sanctions Enforcement

In the past six months, U.S. authorities reached two large settlements with international financial institutions for violations of U.S. sanctions regulations. The underlying conduct involved AML issues as well, most notably the financial institutions' efforts to conceal the involvement of sanctioned parties before routing payments through the U.S. financial system. The U.S. Government used money laundering charges to bolster the strength of their case, and to increase the fine amounts.

- **Standard Chartered Bank Agreed to Pay More than 1 Billion Dollars to Resolve Iran Sanctions and AML Charges.** In April 2019, the London-based financial institution Standard Chartered Bank (SCB) reached agreements with the [Department of Justice](#) (DOJ), the [Federal Reserve](#), the [U.S. Department of the Treasury's Office of Foreign Assets Control](#), the [NYDFS](#), and the [Manhattan District Attorney's Office](#) to settle allegations that it had processed thousands of financial transactions through U.S. financial institutions on behalf of Iranian entities, in violation of U.S. sanctions on Iran. OFAC's enforcement information also notes apparent violations of the now-repealed Burmese Sanctions Regulations (BSR), the Cuban Assets Control Regulations

(CACR), the now-repealed Sudanese Sanctions Regulations, the Syrian Sanctions Regulations (SSR), and the Zimbabwe Sanctions Regulations (ZSR). Separately, SCB reached an agreement with the U.K. [Financial Conduct Authority](#) (FCA) to pay a fine of approximately 100 million pounds sterling due to "serious and sustained shortcoming" in the bank's AML controls. Total penalties and forfeiture with all relevant enforcement authorities surpassed 1.3 billion dollars.

- **UniCredit Bank AG and Affiliates Agreed to Pay 1.3 Billion Dollars to Resolve Iran Sanctions Charges.** In April 2019, UniCredit Bank AG (UCB AG) reached agreements with the [DOJ](#), the [Federal Reserve](#), [OFAC](#), the [NYDFS](#), and the [Manhattan District Attorney's Office](#) to settle allegations that it had processed transactions that violated U.S. sanctions in connection with Iran. Better known by its trade name Hypovereinsbank, the Munich-headquartered financial institution allegedly "went to great lengths" to assist the Islamic Republic of Iran Shipping Lines (IRISL) in routing payments through the U.S. financial system, often by concealing IRISL's involvement in a transaction. IRISL is currently subject to U.S. sanctions for its alleged role in Iran's nuclear proliferation efforts. UCB AG's parent UniCredit SpA and sister company UniCredit Bank Austria (BA) also reached agreements with the DOJ. No AML charges were brought, despite the UCB AG's apparent role in concealing IRISL's involvement in certain financial transactions. Total penalties and forfeiture with all relevant enforcement authorities surpassed 1 billion dollars.

Actions Against Individuals

A recent decision from the Ninth Circuit clarified that the application of money laundering statute 18 U.S.C. § 1957 in instances of bribery as the predicate offence was not limited to the requirements of domestic bribery statute 18 U.S.C. § 201.

Other recent developments included a Consent Order and civil money penalty against the former General Counsel of Rabobank for concealing information from the OCC and a guilty plea by a former Wells Fargo banker for conspiring to launder money through Wells Fargo accounts.

- **Ninth Circuit Rules that Money Laundering Statute Is Not Restricted to Domestic Bribery Rules.** In August, the Ninth Circuit [upheld](#) the conviction of former South Korean seismologist Heon-Cheol Chi and ruled that the money laundering statute under which he was convicted is not restricted to domestic bribery statute 18 U.S.C. § 201. Mr. Chi was charged with laundering over 1 million dollars in bribes from two seismology companies, Guralp Systems in the U.K. and Kinometrics in the U.S. In return for the payments, Mr. Chi allegedly helped ensure that the government-funded geological research institute at which he was employed purchased products from the two companies and gave the companies inside information about their competitors. In 2017, a federal jury convicted Mr. Chi of one count of laundering bribe money under 18 U.S.C. § 1957, which criminalizes engaging in monetary transactions over 10,000 dollars derived from certain "offense[s] against a foreign nation," including crimes involving "bribery of a public official" under 18 U.S.C. § 1956. Mr. Chi argued on appeal that the district court erred in concluding that "bribery of a public official" included a violation of the South Korean Criminal Code and instructing the jury to that effect. The Ninth Circuit disagreed, holding that the district court did not err in its instruction. The Ninth Circuit thus rebuffed a narrow reading of the money laundering statute and found that the statute does not require a violation of U.S. bribery law.
- **OCC Issues Consent Order and Civil Money Penalty Against Former General Counsel of Rabobank, N.A.** In July 2019, the OCC [issued](#) a consent order of prohibition and 50,000 dollars civil money penalty against Daniel Weiss, the former General Counsel of Rabobank, N.A. The [notice of charges](#) alleges that Mr. Weiss made false statements to the OCC in violation of 18 U.S.C. § 1001 and concealed bank documents in violation of 12 U.S.C. § 481. The notice specifically alleges that Mr. Weiss submitted a response to the OCC on behalf of Rabobank that failed to acknowledge the existence of a third-party report, which allegedly corroborated the OCC's examination findings that Rabobank's BSA/AML compliance program was ineffective. A whistleblower later alerted the OCC to the third-party report. Mr. Weiss was terminated by Rabobank in September 2015 following an internal investigation, which found that Mr. Weiss had concealed the report from the OCC and had made repeated false statements to the OCC. The [consent order](#) prohibits Mr. Weiss from participating in the affairs of any federally insured depository institution and assesses 50,000 dollars for violations of law and unsafe or unsound practices.

In February 2018, Rabobank pled guilty to conspiracy to obstruct an OCC examination and agreed to pay a forfeiture for 368,701,259 dollars and a civil money penalty to the OCC for 50 million dollars.

- **Wells Fargo Personal Banker Pleaded Guilty in Money Laundering Scheme.** In May 2019, Wells Fargo personal banker Luis Fernando Figueroa, of Tijuana, Mexico, pleaded guilty to money laundering charges. Mr. Figueroa admitted to conspiring with others to launder and transfer money to Mexico through accounts he opened at Wells Fargo. According to the [press release](#) from the U.S. Attorney's Office for the Southern District of California, an international money laundering organization based in Mexico and operating primarily in San Diego, recruited "couriers" who traveled to various U.S. cities to pick up and transport up to hundreds of thousands of dollars in narcotics proceeds. The international organization also recruited individuals at U.S. banking institutions to open personal bank accounts into which the couriers deposited the money. The money was then transferred from the accounts via international wire transfers to Mexican shell companies operated by the international organization. When the funds reached Mexico, they were transferred to representatives of the Sinaloa Cartel, a Mexican-based drug trafficking organization. Six former members of the money laundering organization have also pleaded guilty. Mr. Figueroa faces up to 20 years imprisonment and a 500,000 dollar fine.

Cryptocurrency

U.S. enforcement agencies continue to regulate cryptocurrency through new guidance and an appeal for whistleblowers, and to take action against individuals alleged to have violated cryptocurrency regulations.

- **AML Organization Announces New Guidance for Cryptocurrency Compliance.** In June 2019, the independent, inter-governmental Financial Action Task Force (FATF) issued two important pieces of guidance that impose anti-money laundering reporting requirements on virtual asset service providers (VASPs). The FATF issued an [interpretive note](#) to Recommendation No. 15 of FATF's Recommendations, which relates to virtual assets. At the same time, FATF also published "[Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers](#)."

Both the interpretive note and the guidance make clear that VASPs should implement the anti-money laundering recommendations that previously applied to traditional financial institutions. Thus, under the new FATF guidance, virtual currency providers will be required to share with other financial institutions the identity of those who send and receive cryptocurrency, conduct due diligence and know-your-customer analysis, and develop risk-based compliance programs. U.S. Treasury Secretary Steven Mnuchin that the new guidance "will enforce a level playing field for virtual asset service providers, including cryptocurrency providers, and traditional financial institutions." Mnuchin noted, "This will enable the emerging FinTech sector to stay one-step ahead of rogue regimes and sympathizers of illicit causes searching for avenues to raise and transfer funds without detection."

As reported in the [press](#), executives at cryptocurrency firms have complained that the industry does not currently have the appropriate infrastructure to transmit customer information.

- **US Government Announces Successful Enforcement Actions Against Individuals.** In April 2019, the U.S. government announced the results of two enforcement actions against individuals involved in cryptocurrency violations, one resulting in a two-year prison sentence and another resulting in a civil penalty from FinCEN:
 - Bitcoin dealer Jacob Burrell Campos was [sentenced](#) to two years in prison and was ordered to forfeit 823,357 dollars in illegal profits for operating an unlicensed money transmitting business. Burrell, who was [indicted](#) in August 2018 and pled guilty two months later, admitted that he operated a Bitcoin exchange without registering with the Financial Crimes Enforcement Network (FinCEN) or implementing required anti-money laundering programs.
 - FinCEN [assessed](#) a civil money penalty of 35,350 dollars against Eric Powers for willfully violating the registration, program, and reporting requirements of the Bank Secrecy Act. In its assessment, FinCEN determined that Powers conducted more than 1,700 transactions between December 6, 2012 and September 24, 2014, and was required but failed to register as a money

services business. Powers also violated regulations that required him, as a money services business, to (1) develop, implement, and maintain an effective AML program; (2) file suspicious activity reports; and (3) file currency transaction reports. FinCEN took into account other penalties imposed upon Powers by state and federal agencies, including 123,192.14 dollars and 237.53575 bitcoins that were [forfeited](#) by Powers in a civil case against Powers in the District of Maryland in 2015.

- **CFTC Solicits Whistleblowers for Cryptocurrencies.** In May 2019, the Whistleblower Office for the Commodity Future Trading Commission (CFTC) issued an [alert](#) seeking whistleblowers for cryptocurrency issues. The alert, which was issued along with other alerts regarding whistleblowing for potential insider trading, Foreign Corrupt Practices Act, and Bank Secrecy Act violations, explained the system for receiving monetary awards for tips that lead to successful enforcement actions and highlighted the types of misconduct the CFTC is concerned with, including price manipulation, unregistered platforms, and supervision failures.
- **Cryptocurrency Exchange Receives Regulatory Approval and Reaches Out to Retail Investors, Advertising Stability and Regulation.** Starting in January 2019, cryptocurrency exchange Gemini Trust Company, LLC started an out-of-home advertising campaign touting itself as "The Regulated Cryptocurrency Exchange." The advertising campaign, which featured advertisements in subway stations, taxi cabs, and newspapers, was one of the first campaigns directed at retail investors, according to press [reports](#). Gemini went live in October 2015, and in May 2016, New York Governor Andrew Cuomo [announced](#) that the New York State Department of Financial Services authorized Gemini as the first licensed trader of the cryptocurrency Ether. In September 2018, Gemini [received](#) regulatory approval for the Gemini dollar, which is pegged to the U.S. dollar.

Update on International Money Laundering Scandals

Danske Bank Scandal

There have been several notable developments in the Danske Bank money laundering scandal.

- **Danske Bank's Regulators in Denmark and Estonia still under Investigation by the EU** . The European Commission continues its investigation into the role Danske Bank's regulators in Denmark and Estonia have played in the multi-billion money laundering scandal involving the bank. The investigation may lead the EU to initiate a so-called "infringement procedure," which may expose both countries to court proceedings and potential financial penalties if they are found to have breached EU law.
- **Authorities Raid Headquarters of Nordea Bank and Deutsche Bank** . On June 12, 2019, Denmark's state prosecutor searched Nordea Bank's headquarters in Copenhagen. According to Finnish [broadcaster](#) Yli, Nordea Bank allegedly handled 790 million dollars in suspicious transactions between 2005 and 2017. In April 2019, Nordea Bank took a 95 million euro accounting provision for a possible fine for its alleged role in the money laundering.

On September 24, 2019, German authorities [raided](#) Deutsche Bank's headquarters in Frankfurt in connection with their investigation into whether Germany's biggest bank had facilitated transfers of illicit funds from Danske Bank and whether it had failed to alert authorities about suspicious transactions

- **Former Head of Danske Bank Commits Suicide.** On September 25, 2019, Bloomberg [reported](#) that Aivar Rehe, the former head of Danske Bank in Estonia, had been found dead after disappearing from his home in Tallinn two days before. Rehe's death was later [ruled](#) a suicide by the Estonian Prosecutor General's Office. Rehe, who was at the helm of Danske Bank's Estonian branch from 2008 to 2015, was not a suspect in the laundering probe, nor was he among the group of ten Estonian bankers that had been detained by the police in 2018 in connection with the probe and charged with money-laundering.
- **More Claimants File Lawsuits against Danske Bank** . It was [reported](#) on October 22, 2019 that between October 16-18, 2019, an additional 64 institutional investors filed lawsuits against Danske Bank, accusing Denmark's largest bank and its senior management of participating in the Russian money laundering scheme and concerted cover-up and asserting 800 million in economic damages. This brings the total number of institutional investor and other plaintiffs in the Danske Bank litigation to 232.

Investigation of Swedbank

- **Swedbank waives attorney-client privilege over specific internal reports** . On September 17, 2019, Swedbank [agreed](#) to allow the Swedish Economic Crime Authority (EBM) to interview one of Swedbank's external lawyers who prepared reports for the bank related to its internal controls and allegations of money laundering. Swedbank said it would waive attorney-client privilege and give EBM access to documents from Erling Grimstad at the Norwegian law firm of Advokatfirmaet Erling Grimstad AS. The documents relate to Grimstad's "assignments for Swedbank" and to internal investigation of the bank's compliance with local AML laws.
- As we [reported](#) in our previous edition of AML Enforcement Trends, Swedbank has been under investigation by authorities in Sweden, some of the Baltics states, including Estonia, and the United States for allegations that Swedbank accounts in Estonia may have been used for money-laundering involving transfers of approximately 4.3 billion dollars in suspicious transactions between Swedbank and Danske Bank's Estonian unit between 2007 and 2015. Swedbank had hired Norwegian lawyer Grimstad to prepare reports on the allegations and its internal systems to prevent money laundering.
- In its [press release](#) from September 17, 2019, Swedbank also said that it had responded to questions from the Financial Supervisory Authorities in Sweden and Estonia. The bank also said that its AML work still had "certain shortcoming" and that it was working "to ensure regulatory compliance going forward." An investigation initiated by the bank earlier in 2019 is expected to be completed in early 2020, according to the press release.

Spotlight on Brazil

Recently, Brazilian authorities arrested three executives from Brazilian bank Banco Paulista S.A. in connection with a corruption and money laundering scheme investigated under the Lava Jato/Car Wash investigations. Brazil alleged that, from 2009 to 2015, Banco Paulista was part of a money laundering scheme valued at up to R328 million dollars (83 million U.S. dollars). The alleged scheme involved Meinel Bank Ltd, a lender that Odebrecht owned in Antigua and Barbuda between 2010 and 2016.

However, on July 16, 2019, Brazil's Supreme Court issued a [decision](#) suspending criminal investigations that use detailed financial data from government entities without judicial authorization. This decision was issued at the request of Senator Flávio Bolsonaro (son of Jair Bolsonaro, the current President of Brazil) and it halted most of the country's money laundering investigations based on confidential data shared by the Financial Activities Control Council (COAF) and the Federal Treasury without prior authorization from a court. The decision put the effectiveness of COAF fighting money laundering crimes at risk and represents an unexpected step backwards for enforcement in Brazil.

COAF has played a relevant role in fighting AML, producing reports on financial transactions considered atypical – not necessarily illegal – and sharing information with Brazilian authorities. In the last years, COAF financial intelligence reports have been critical in investigations, financial intelligence provided by the Agency subsidized major anti-corruption operations in Brazil, such as "Zealots" and Lava Jato/Car Wash.

In February 2019, President Bolsonaro's administration changed the status of the COAF, creating two new bodies within COAF: Financial Intelligence and Supervision Boards. The change in COAF was been widely debated in the Brazilian media and experts are divided on whether the decision will enhance or harm COAF's role in combatting money laundering. Despite recent legislative changes in the country, the FATF issued a [statement](#) conveying its concerns about Brazil's delays in implementing recommendations in combating money laundering. FATF also announced that it continues to see the delay as a membership issue that it will consider during the October 2019 plenary meeting.

The Brazilian Supreme Court is scheduled to pick up the matter again in late November. Until then, Brazil may be losing territory in combatting money laundering.

Editors: Ann Sultan, William P. Barry, Kirby D. Behre

Contributors: Collmann Griffin, Nina C. Gupta,* Ian A. Herbert, Ivo K. Ivanov,* Elizabeth J. Jonas, Maryna Kavaleuskaya,* Bruno Pandini,** Chervonne Colón Stevenson*

**Former Miller & Chevalier attorney*

**Former Miller & Chevalier law clerk*

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.