2017 Anti-Money Laundering Review and 2018 Outlook

Last year, financial regulators around the world imposed more than $2 billion in fines related to anti-money laundering ("AML") compliance failures. With AML enforcement shifting into a higher gear, financial institutions need a comprehensive picture of regulatory priorities so they can effectively build their compliance functions.

To assist financial institutions in this effort, the Debevoise Banking Group has compiled the *2017 Anti-Money Laundering Review and 2018 Outlook*, summarizing 19 AML enforcement actions initiated or concluded in 2017. The report identifies three key AML enforcement trends:

Debevoise & Plimpton

- **An increased inclination by regulators to hold compliance officers and other employees personally liable for compliance failures.**
- **The continued assertion by New York State's Department of Financial Services of a prominent role in AML enforcement.**
- **Notable AML enforcement activity outside of the United States.**

We hope that you find the *2017 Anti-Money Laundering Review and 2018 Outlook* to be a helpful reference guide and we look forward to discussing AML developments and best practices at your convenience.

Table of Contents

Executive Summary

Enforcement of anti-money laundering ("AML") regulations continued to be rigorous in 2017, with federal regulators and prosecutors in the United States imposing AML penalties totaling more than $1 billion, and state and foreign jurisdictions levying an additional $1 billion. As we survey the AML enforcement actions initiated or concluded around the world last year, three trends were particularly notable:

Regulators focused on personal liability. A federal court ruled that the Bank Secrecy Act ("BSA") permitted the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") to seek civil penalties against the former chief compliance officer of a financial institution for willful violations of the BSA and, in separate actions, FinCEN, the Securities and Exchange Commission and the Federal Deposit Insurance Corporation each imposed monetary penalties and industry employment prohibitions on financial institution employees for their role in AML compliance failures.[1] With personal liability having been confirmed by the court, we expect an increase in such actions going forward.

1 *See Thomas Haider (MoneyGram) at* page 9; Banamex USA (Citigroup) at 5; Alexander Vinnik (BTC-e) at 7; John Telfer (Meyers Associates L.P.) at 17.

Continued on page 3

Executive Summary (Continued)

New York State continued to aggressively assert its role in AML enforcement. The New York State Department of Financial Services ("DFS") concluded enforcement actions against three international banks resulting in penalties totaling $661 million, representing approximately 40 percent of the total AML penalties imposed by agencies within the United States. In addition, DFS filed two federal lawsuits against the Office of the Comptroller of the Currency ("OCC") claiming, in essence, that the OCC was wrongfully encroaching upon its regulatory domain. While one lawsuit was dismissed as being premature, we expect the issue to be relitigated in due course, given that these actions appear to be skirmishes in a larger turf war.[2]

AML regulation and enforcement expanded globally. Regulators in Australia and the United Kingdom brought AML enforcement actions which resulted in the imposition of record-setting penalties, and the French National Financial Prosecutor concluded a tax and money laundering investigation of a private bank by imposing penalties under a new procedure modeled on U.S. deferred prosecution agreements. Success by foreign jurisdictions in AML enforcement will lead to further action and possibly the emergence over time of more coordinated international efforts.[3]

Finally, our review includes discussions of some of 2017's rule-making milestones, including the DFS's Rule 504, the Department's landmark anti-money laundering regulation,[4] and the European Union's Fourth Anti-Money Laundering Directive, which member states were required to fully implement by midyear.[5]

2 *See* DFS Opposition to the OCC's Proposal to Create a New National Bank Charter for "FinTech" Companies at page 14; DFS Opposes MUFG's Switch to an OCC National Charter at page 16.
3 *See* International at page 19.
4 *See* Part 504 Anti-Money Laundering Regulation Goes into Effect at page 11.
5 *See* Regulations Based on European Union's Fourth Anti-Money Laundering Directive Come into Full Force at page 22.

Enforcement Actions and Related Developments

Department of Justice

Western Union

(Multiple criminal investigations lead to focus on MSB's prior AML and fraud compliance deficiencies; $586 million forfeiture.)

On January 19, 2017, Western Union agreed to forfeit $586 million in restitution to victims of fraud to resolve investigations by the United States Department of Justice ("DOJ"), the Federal Trade Commission ("FTC") and FinCEN. Announced on the last day of the Obama administration, these

Continued on page 4

Western Union (Continued)

coordinated enforcement actions resulted in the largest AML monetary penalty levied by the United States in 2017.

In a Deferred Prosecution Agreement ("DPA")[6] with the DOJ's Money Laundering and Asset Recovery Section and four U.S. Attorneys' Offices,[7] Western Union admitted to criminal violations from 2004 to 2012 that included willfully failing to maintain an effective AML program, and aiding and abetting wire fraud. As part of the DPA, the DOJ acknowledged that subsequent to September 2012, Western Union had implemented compliance enhancements to improve its anti-fraud and AML programs.

Western Union simultaneously entered into a stipulated order without admitting fault with the FTC in order to resolve the FTC's allegations that Western Union failed to take effective measures to mitigate fraud in the processing of money transfers sent by consumers. As part of this stipulated order and in addition to the $586 million forfeiture, Western Union agreed to the appointment of an independent compliance auditor to ensure, among other things, that appropriate due diligence would be conducted on existing and prospective Western Union agents, and that necessary steps would be taken to monitor and investigate agent activity.

In conjunction with the FTC stipulated order and the DPA with the DOJ, FinCEN assessed a $184 million penalty, which was deemed satisfied by the $586 million forfeiture.[8] Western Union consented to FinCEN's determination that prior to 2012, the company willfully violated AML requirements by failing to implement and maintain an effective, risk-based AML program and by failing to file timely suspicious activity reports ("SARs").

These enforcement actions arose out of several different criminal investigations involving alleged (i) consumer fraud activity targeting victims in Pennsylvania,[9] (ii) transactions sent from California to China that were structured to avoid reporting obligations under the Bank Secrecy Act ("BSA")[10] and (iii) the transmission of sports gambling bets from Florida to locations in Costa Rica.[11] Besides the magnitude of the forfeiture levied in this case, the enforcement actions against Western Union were notable for the government's recognition that the apparent violations had ended five years prior in 2012.[12]

---

6 *U.S. v. The Western Union Co.*, Deferred Prosecution Agreement, 1:17-cr-00011-CCC (M.D. Pa. Jan. 19, 2017) [hereinafter *DPA*], *available* here.

7 The U.S. Attorney's Offices for the Middle and Eastern Districts of Pennsylvania, the Central District of California, and the Southern District of Florida.

8 Press Release, FinCEN, FinCEN Fines Western Union Financial Services, Inc. for Past Violations of Anti-Money Laundering Rules in Coordinated Action with DOJ and FTC (Jan. 19, 2017), *available* here.

9 DPA at 6. In the DPA, prosecutors alleged that Western Union knew that certain of its agents were complicit in the schemes perpetrated by fraudsters who were using the agents' locations to receive payments from victims.

10 DPA at 19.

11 DPA at 27.

12 DPA, Attachment A: Statement of Facts, at 29.

Banamex USA (Citigroup)

(18,000+ surveillance alerts result in less than 10 investigations and nine SARs; $97.44 million forfeiture.)

On May 19, 2017, Los Angeles-based Banamex USA ("Banamex"), a subsidiary of Citigroup Inc., agreed to forfeit $97.44 million and entered into a non-prosecution agreement ("NPA") with the DOJ. Banamex admitted to criminal violations by willfully failing to maintain an effective AML compliance program and willfully failing to file SARs.

According to the NPA and the accompanying statement of facts,[13] Banamex partnered with and provided services to numerous money service businesses ("MSBs") in the United States to facilitate the transfer of money remittances primarily to Mexico, but in doing so, went beyond providing the typical bank account services generally offered to MSBs. Among other things, Banamex provided the data transfer technology to transmit transactional data from the originating MSB agent to the paying agent in Mexico and had visibility into each MSB transaction it processed, including information about the sender, beneficiary, amount, pay date, pay location and transaction number.

From approximately 2007 until 2012, Banamex processed more than 30 million remittance transactions to Mexico with a total value of more than $8.8 billion, which generated more than 18,000 alerts on $142 million in potentially suspicious remittance transactions. Despite this volume of transaction activity, Banamex conducted fewer than 10 investigations and filed only nine SARs.

In March 2017, the Federal Deposit Insurance Corporation ("FDIC") announced related enforcement actions against four former senior Banamex executives relating to the bank's BSA violations. The executives named included the CEO and Chairman of Banamex and the Executive Vice President of Corporate and International Banking. As part of those actions, two Banamex executives were fined a total of $160,000 and prohibited from working at financial institutions in the future. One Banamex executive was fined $30,000 and another Banamex executive was prohibited from working at financial institutions in the future.[14]

According to the NPA, Banamex received only partial credit for its cooperation with the DOJ's investigation because its initial efforts to provide relevant facts and documents to the DOJ were neither timely nor substantial. Subsequently, however, Banamex provided cooperation that was substantial, including (i) collecting, analyzing, and organizing voluminous evidence and information, (ii) producing documents from foreign countries in ways that did not implicate foreign data privacy laws and (iii) voluntarily making foreign-based employees available for interviews in the United States.[15]

---

13 U.S. Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section, Banamex USA and Citigroup, Non-Prosecution Agreement (May 18, 2017), *available* here.

14 *See In re Noseworthy*, Order of Prohibition and Order to Pay, 2017 WL 1550287 (F.D.I.C. Feb. 14, 2017), *available* here; *In re Villar*, Order of Prohibition and Order to Pay, 2017 WL 1550285 (F.D.I.C. Feb. 14, 2017), *available* here; *In re Figueroa*, Order to Pay, 2017 WL 1550288 (F.D.I.C. Feb. 14, 2017), *available* here; *In re Moreno*, Order of Prohibition, 2017 WL 1550286 (F.D.I.C. Feb. 14, 2017), *available* here.

15 DPA at 1.

HSBC

(Federal appeals court rules that an independent monitor's report will remain sealed.)

On July 12, 2017, the U.S. Court of Appeals for the Second Circuit ruled that an HSBC independent monitor report would remain sealed, overruling an order from the District Court for the Eastern District of New York to make the report public.[16] The report was the product of the independent monitor whose oversight HSBC agreed to in 2012 as part of its $1.9 billion DPA with the DOJ and other agencies after prosecutors found it allowed money to travel through its network in violation of sanctions and anti-money-laundering laws. The District Court had taken supervisory control over the DPA between the government and HSBC, and had found that the report qualified as a judicial record. The Second Circuit panel held that the monitor report was not a judicial document because it was not relevant to the performance of the judicial function, and that the district court's invocation of supervisory power over the DPA was an impermissible encroachment into the executive branch's domain.

In December 2017, HSBC announced that the DOJ had agreed to release the bank from its DPA based on improvements it has made to its compliance program, and that the independent monitor engagement would terminate in July 2018. The termination of the independent monitor's engagement, reported to be both extensive and contentious, was a significant development for the bank.[17] More broadly, the Second Circuit's decision preventing the release of the independent monitor's earlier report should provide some guidance to both prosecutors and financial institutions when structuring independent monitor engagements.

16 *U.S. v. HSBC Bank*, 863 F.3d 125 (2d. Cir July 12, 2017).
17 *See* Margot Patrick, "HSBC to Be Released from U.S. Deferred Prosecution Agreement," Wall St. J., (Dec. 11, 2017), *available* here.

Financial Crimes Enforcement Network

Merchants Bank of California

(Violations by a bank specializing in providing service to money services businesses or MSBs, including those owned or managed by bank insiders; $7 million in penalties)

On February 27, 2017, FinCEN announced the assessment of a $7 million civil money penalty ("CMP") against Merchants Bank of California ("Merchants") for willful violations of the BSA, including its failure to (i) establish and implement an adequate AML program, (ii) conduct required due diligence on its foreign correspondent accounts and (iii) detect and report suspicious activity. As a result of its failures, FinCEN asserted that Merchants allowed "billions of dollars" to flow through the U.S. financial system without effective monitoring.[18]

18 Press Release, FinCEN, FinCEN Penalizes California Bank for Egregious Violations of Anti-Money Laundering Laws (Feb. 27, 2017) [hereinafter *FinCEN Press Release*], *available* here.

Continued on page 7

Merchants Bank of California (Continued)

The OCC simultaneously assessed a $1 million CMP for deficiencies related to previous consent orders entered into by Merchants. The payment of the $1 million CMP was to be credited towards the satisfaction of the FinCEN penalty.[19]

In announcing the action, FinCEN's Acting Director noted that "[H]ere we had an institution run by insiders essentially to provide banking services to MSBs that the insiders owned, combined with directions from Bank leadership to staff to ignore BSA requirements with respect to those MSB customers and others."[20]

According to FinCEN, Merchants specialized in providing banking services to check-cashers and money transmitters, and bank insiders owned or managed these MSBs that had accounts at the bank. In several instances, bank insiders allegedly interfered with the BSA staff's attempts to investigate suspicious activity related to these accounts, and at times threatened them with dismissal or other retaliation.[21] Notably, FinCEN did not include bank insiders in its enforcement action, though it noted generally that its settlement with a financial institution does not preclude consideration of separate enforcement actions that may be warranted with respect to individuals.[22] Finally, FinCEN noted that Merchants also failed to provide its BSA officer with the necessary level of authority and independence, and that compliance staff was not empowered with sufficient authority to implement the Bank's AML program.[23]

BTC-e a/k/a Canton Business Corporation and Alexander Vinnik

(Federal indictment of digital currency exchange leads to Treasury's first action against a foreign-located money services business; $122 million in penalties.)

On July 26, 2017, the U.S. Attorney for the Northern District of California announced the indictment of Alexander Vinnik and an organization he allegedly operated, BTC-e, for operating an unlicensed MSB, money laundering and related crimes.[24] FinCEN assessed a $110 million CMP against BTC-e for willfully violating U.S. AML laws and a $12 million CMP against Mr. Vinnik for his role in the violations. This enforcement action marks FinCEN's first action against a foreign MSB.

According to the indictment, BTC-e was founded in 2011 and was one of the world's largest and most widely used digital currency exchanges. The indictment alleges that BTC-e allowed its users to trade in the digital currency "Bitcoin" with high levels of anonymity. As to Mr. Vinnik, the indictment alleges that he received funds from the infamous computer intrusion or "hack" of Mt. Gox—an earlier digital currency exchange that eventually failed, in part due to losses attributable to hacking. The indictment alleges that Mr. Vinnik obtained funds from the illegal hack of Mt. Gox and laundered

19 *Id.*
20 *Id.*
21 *In the Matter of Merch. Bank of Cal.*, Assessment of Civil Money Penalty at 4-5, No. 2017-02 (FinCEN Feb. 16, 2017), *available* here.
22 *See FinCEN Press Release.*
23 *Merch. Bank of Cal.*, at 9-10.
24 Press Release, U.S. Attorney's Office, N. Dist. of Cal., Russian National and Bitcoin Exchange Charged in 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds from Hack of Mt. Gox (July 26, 2017).

Continued on page 8

BTC-e a/k/a Canton Business Corporation and Alexander Vinnik (Continued)

those funds through various online exchanges, including his own BTC-e and a now defunct digital currency exchange, Tradehill, based in San Francisco, California. The indictment alleges that by moving funds through BTC-e, Mr. Vinnik sought to conceal and disguise his connection with the proceeds from the hacking of Mt. Gox and the resulting investigation.

As for defendant BTC-e, the indictment alleged that, despite doing substantial business in the United States, BTC-e was not registered as a money services business with the U.S. Department of the Treasury, had no AML process, no system for appropriate "know your customer" or "KYC" verification and no AML program as required by federal law.

Lone Star National Bank

(Bank reportedly ill-equipped to take on international correspondent banking activities; $2 million penalty.)

On November 1, 2017, FinCEN announced a $2 million CMP against Lone Star National Bank ("Lone Star") of Pharr, Texas for willfully violating the BSA. As noted in FinCEN's assessment, among other lapses, Lone Star failed to comply with section 312 of the USA PATRIOT Act, which imposes specific due diligence obligations with respect to correspondent banking.[25]

According to FinCEN, from May 2010 to November 2011, Lone Star provided U.S. currency bulk cash deposit and another correspondent banking service to a large financial institution headquartered in Mexico, whose name was not disclosed by FinCEN (the "Foreign Bank").[26] During account opening, Lone Star failed to identify the "well known and public information" that the president and principal owner of the Foreign Bank had previously agreed to pay civil penalties to the U.S. Securities and Exchange Commission to resolve allegations of securities fraud.[27] In less than two years, Lone Star allegedly allowed $260 million to flow through the Foreign Bank's account without sufficient controls in place to detect and report suspicious activity.[28]

FinCEN noted that many of the lapses in Lone Star's BSA compliance were previously covered in an earlier action by the OCC,[29] but that its action, which focused on Lone Star's section 312 violations, specifically highlighted the need for a financial institution to avoid taking on international business for which it is not prepared.[30]

---

25 *In the Matter of Lone Star Nat'l Bank*, Assessment of Civil Money Penalty, No. 2017-04 (FinCEN Oct. 27, 2017), *available* here.
26 *Id.* at 5.
27 *Id.* at 6.
28 *Id.* at 5.
29 *Id.* at 10-11. The OCC entered into a Consent Order and a Memorandum of Understanding with Lone Star in 2012. Lone Star allegedly continued to have programmatic anti-money laundering ("AML") deficiencies and in 2015, the OCC issued a Consent Order for a Civil Money Penalty in the amount of $1 million. As a result of subsequent remedial measures taken by Lone Star to improve its BSA program, the OCC terminated the Consent Order on July 27, 2017. Lone Star's previous penalty payment to the OCC was credited to FinCEN's assessment and the bank was required to pay an additional $1 million to satisfy its obligation to FinCEN.
30 Press Release, FinCEN, FinCEN Penalizes Texas Bank for Violations of Anti-Money Laundering Laws Focusing on Section 312 Due Diligence Violations (Nov. 1, 2017), *available* here.

Artichoke Joe's Casino

(Gaming industry card club fails to file SARs on loan-sharking and other illicit activities; $8 million penalty.)

On November 17, 2017, FinCEN announced an $8 million CMP against Artichoke Joe's Casino ("AJC"), a California corporation doing business as Artichoke Joe's Casino, for its willful violation of AML laws.[31] AJC is a card club, in operation since 1916 and offering card and tile games, and a "financial institution" and "card club" within the meaning of the BSA.[32] According to FinCEN's assessment, during the eight-year period from October 2009 to November 2017, AJC failed to implement and maintain an effective AML program, and failed to detect and timely report suspicious transactions.

FinCEN noted that AJC was the subject of a raid in 2011 by state and federal law enforcement which led to the racketeering indictment and conviction of AJC customers for loan-sharking and other illicit activities. The investigation established that AJC employees knew that loan-sharks were conducting criminal activity through the card club. Loan-sharks, who extended extortionate and unlawful credit to AJC patrons, allegedly conducted illicit transactions using the card club's gaming chips and U.S. currency.[33]

According to FinCEN, AJC failed to file any SARs on this activity and subsequently failed to adopt policies and procedures to address the risks associated with gaming practices that allow customers to pool or commingle their bets with relative anonymity.[34]

Thomas Haider (MoneyGram)

(Settlement of BSA claims against a former Chief Compliance Officer; $250,000 penalty.)

On May 4, 2017, FinCEN and the U.S. Attorney's Office for the Southern District of New York announced the settlement of claims under the BSA against Thomas E. Haider, the former Chief Compliance Officer of MoneyGram International, Inc. Mr. Haider agreed to a three-year injunction barring him from performing a compliance function for any money transmitter and agreed to pay a $250,000 penalty.[35]

In 2012, MoneyGram entered into a DPA with the DOJ for, among other offenses, willfully failing to implement an effective AML program under the BSA. In conjunction with the DOJ's investigation, MoneyGram was also investigated by FinCEN, which ultimately did not take action against MoneyGram itself. However, on December 8, 2014, FinCEN issued a $1 million civil penalty against Mr. Haider and sought to bar him from employment at any U.S. financial institution.[36]

FinCEN argued that Mr. Haider was personally responsible for MoneyGram's AML compliance failures. Specifically, FinCEN alleged that Mr. Haider did not (i) implement discipline or termination policies for agents and outlets suspected of engaging in, or presenting an unreasonable risk of, fraud

31 *In the Matter of Artichoke Joe's*, Assessment of Civil Money Penalty, No. 2017-05 (FinCEN Nov. 15, 2017), *available* here.
32 *Id.* at 2, *see also* 31 U.S.C. § 5312(a)(2)(X); 31 C.F.R. § 1010.100(t)(6).
33 *Id.* at 4.
34 *Id.* at 5.
35 Press Release, FinCEN, FinCEN and Manhattan U.S. Attorney Announce Settlement with Former MoneyGram Executive Thomas E. Haider (May 4, 2017), *available* here.
36 Press Release, FinCEN, FinCEN Assesses $1 Million Penalty and Seeks to Bar Former MoneyGram Executive from Financial Industry (Dec. 8, 2014), *available* here.

Continued on page 10

Thomas Haider (MoneyGram) (Continued)

or money laundering, (ii) ensure individuals responsible for filing SARs were given proper access to information known by MoneyGram's Fraud Department or (iii) conduct due diligence or effective audits of MoneyGram agents and outlets, including those known to be or suspected of engaging in fraud or money laundering. FinCEN alleged that, as a result of Mr. Haider's failures, agents and outlets known or suspected by MoneyGram personnel to engage in fraud or money laundering were permitted to use MoneyGram as a money transfer system to facilitate their schemes.

Mr. Haider filed a motion in the District Court of Minnesota, arguing *inter alia* that FinCEN lacked the power to take such personal action against him. But on January 8, 2016, the court ruled in favor of FinCEN,[37] finding that the general civil liability provisions of the BSA[38] permitted FinCEN to seek civil penalties against a "partner, director, officer, or employee" of a financial institution for willful violations of the BSA, including the obligation on financial institutions to implement an AML program. The court further stated that "Section 5321(a)(1)'s explicit reference to 'partner[s], director[s], officer[s], and employee[s]' demonstrates Congress' intent to subject individuals to liability in connection with a violation of any provision of the BSA or its regulations, excluding the specifically excepted provisions."[39]

FinCEN Revised GTO – Shell Companies Purchasing Luxury Properties

On August 22, 2017, FinCEN issued a revised Geographic Targeting Order ("GTO") requiring U.S. title insurance companies to collect and report information about the natural persons behind shell companies used to buy luxury residential real estate in seven metropolitan areas.40 The GTO is an effort to curb the use of the real estate market as a vehicle to launder illicit proceeds.

The covered transactions are those in which a legal entity purchases residential real estate in any of seven major metropolitan areas with a purchase price exceeding the dollar amount threshold for the given area without using external financing and by using cash, check, money order or a funds transfer. The covered metropolitan areas and the respective dollar thresholds are: Bexar County in Texas ($500,000); Miami-Dade, Broward or Palm Beach counties in Florida ($1,000,000); Brooklyn, Queens, Bronx or Staten Island in New York City ($1,500,000); San Diego, Los Angeles, San Francisco, San Mateo and Santa Clara Counties in California ($2,000,000); Manhattan ($3,000,000); and Honolulu, Hawaii ($3,000,000).

FinCEN Advisory – Corrupt Venezuelan Money Flowing to the United States

On September 20, 2017, FinCEN issued an advisory to financial institutions of widespread public corruption in Venezuela due to the rupture of democratic and constitutional order by the government, and the methods Venezuelan political figures and their associates may use to move and hide proceeds of their corruption.[41] The advisory describes financial red flags to help identify and report activity that may be indicative of corruption.

---

37 *U.S. Dep't of the Treasury v. Haider*, Order Denying Motion to Dismiss, No. 15-CV-01518, 2016 WL 107940 (D. Minn. Jan. 8, 2016).

38 31 U.S.C. § 5321(a).

39 *Haider*, 2016 WL 107940, at 3.

40 FinCEN, Geographic Targeting Order (Aug. 22, 2017), *available* here; Press Release, FinCEN, FinCEN Targets Shell Companies Purchasing Luxury Properties in Seven Major Metropolitan Areas (Aug. 22, 2017), *available* here.

41 Press Release, FinCEN, Reports from Financial Institutions Are Critical to Stopping, Deterring, and Preventing the Proceeds Tied to Suspected Venezuelan Public Corruption from Moving Through the U.S. Financial System (Sept. 20, 2017), *available* here.

FinCEN Information Exchange

On December 4, 2017, FinCEN launched the "FinCEN Exchange" program, designed to enhance information sharing with financial institutions.[42] Under this new program, FinCEN will coordinate closely with law enforcement and convene regular briefings with financial institutions to exchange information on priority illicit finance threats, including targeted information and broader typologies. Private sector participation is completely voluntary and the program does not introduce any new regulatory requirements.

42 Press Release, FinCEN, FinCEN Launches "FinCEN Exchange" to Enhance Public-Private Information Sharing (Dec. 4, 2017), *available* here.

New York State Department of Financial Services

Part 504 Anti-Money Laundering Regulation Goes into Effect

The DFS began the year on January 5, 2017 by reminding financial institutions that Rule 504, the Department's landmark anti-money laundering regulation, went in effect several days earlier on January 1.[43] As discussed in earlier Debevoise client updates,[44] the DFS's Part 504 regulation requires a covered institution to maintain a transaction monitoring program reasonably designed to monitor transactions for potential BSA/AML violations and suspicious activity, and a filtering program reasonably designed to interdict transactions prohibited by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC").

Covered institutions also must adopt either an annual board resolution or a senior officer compliance finding to certify compliance with the regulation. The first such certifications are due by April 15, 2018.

The DFS's press release also provided its AML regulatory scorecard, noting that in the short time since DFS Superintendent Maria T. Vullo had been confirmed as department head in June of 2016, the agency had brought three significant enforcement actions for violations of AML laws (Intesa Sanpaolo S.p.A., which was fined $235 million; Agricultural Bank of China, which was fined $215 million; and Mega Bank of Taiwan, which was fined $180 million).[45]

43 Press Release, NYDFS, New York's Landmark Anti-Terrorism Transaction Monitoring and Filtering Program Regulation Takes Effect (Jan. 5, 2017), *available* here.

44 *See* Client Update, Debevoise & Plimpton LLP, NYDFS Issues Final Anti-Money Laundering and Sanctions Rule (July 6, 2016), *available* here; Client Update, Debevoise & Plimpton LLP, NYDFS Proposes New Anti-Money Laundering Requirements, Liability for Compliance Officers (Dec. 7, 2015), *available* here.

45 The Mega Bank fine was listed in the press release as $185 million instead of the $180 million recited in the original order, *available* here.

Deutsche Bank I[46]

(Failure to report a suspicious $10 billion Russian "mirror-trading" scheme leads to $629 million in penalties.)

On January 30, 2017, Deutsche Bank AG and its New York branch (together "Deutsche Bank") agreed to pay a $425 million fine as part of a consent order with DFS for alleged violations of AML laws involving a "mirror-trading" scheme that allegedly allowed a group of individuals and entities to improperly transfer more than $10 billion out of Russia.47 In a related action involving the same alleged scheme, the UK Financial Conduct Authority ("FCA") fined Deutsche Bank an additional $204 million (£163,076,224), which according to the FCA was the largest financial penalty for AML violations ever imposed by that agency or its predecessor, the Financial Services Authority.48 These enforcement actions are notable for the scope of the alleged activity ($10 billion), the absence of specific allegations that these funds involved criminal conduct49 and the size of the resulting fines ($629 million).

According to the DFS consent order, the trading scheme was conducted through the securities desk of Deutsche Bank's affiliate in Moscow ("DB Moscow"). Certain client companies issued orders to DB Moscow to purchase Russian blue chip stocks, paying in rubles. Shortly thereafter, a related entity would sell the same Russian blue chip stock in the same quantity and at the same price, settling in U.S. dollars, through Deutsche Bank's London branch. A "remote booking function" allowed the DB Moscow trading desk to book both trades, mostly executed by a single trader representing both sides of the transaction. The resulting U.S. dollar payments flowed through Deutsche Bank's New York branch.

While noting that offsetting trades are not inherently illegal, the DFS asserted that none of the suspicious trades "demonstrated any legitimate economic rationale."[50] The buying and selling of securities were conducted by at least 12 entities that were closely related, "linked, for example, by common beneficial owners, management, or agents."[51] The DFS also identified suspicious "one-legged" trades that it says may have involved a second financial institution to execute the other leg. According to the DFS, these one-legged trades were almost entirely buy transactions involving the same counterparties involved in the mirror trades.[52]

---

46 As we discuss below, on May 30, 2017, the Federal Reserve Board ("FRB") announced it would impose a $41 million penalty and enter into a consent order with Deutsche Bank AG ("Deutsche Bank II") for AML deficiencies that touch on the same issues addressed in the January 2017 enforcement action by DFS discussed in this section.

47 *In re Deutsche Bank*, Consent Order, 2017 WL 735666 (N.Y. Bnk. Dept. Jan. 30, 2017), *available* here [hereinafter *Consent Order*]. Pursuant to the consent order, the bank was also required to engage an independent monitor to conduct a review of the bank's existing BSA/AML compliance programs, policies and procedures governing activities by or through its U.S. subsidiary (Deutsche Bank Trust Company of the Americas) and the New York branch.

48 Press Release, FCA, FCA fines Deutsche Bank £163 Million for Serious Anti-Money Laundering Control Failings (Jan. 31, 2017), *available* here.

49 DFS alleged that the $10 billion was "laundered out of Russia" and "could have been used to facilitate money laundering or enable other illicit conduct" but did not offer a further explanation regarding the source of the funds. Press Release, DFS, DFS Fines Deutsche Bank $425 Million for Russian Mirror-Trading Scheme (Jan. 30, 2017), *available* here. Russia's Central Bank has since reported that Deutsche Bank was not the only bank found to have conducted "mirror trades" in recent years, and explained that such trades rank among the largest mechanisms for moving money out of Russia. *See* Evgenia Pismennaya, "Deutsche Bank Wasn't Only 'Mirror' Trader: Russian Central Bank," Bloomberg (June 27, 2017), *available* here.

50 Consent order, at 5.

51 *Id.* at 6.

52 *Id.* Based on the alleged scheme, the additional transactions suggested by DFS, if they occurred, were presumably sell transactions.

Continued on page 13

Deutsche Bank I (Continued)

Overall, the DFS credited Deutsche Bank with ultimately self-identifying and reporting the issue,[53] but faulted the bank for missing numerous opportunities to detect, investigate and stop the scheme through its AML program.[54] Specifically, the DFS alleged that Deutsche bank had (i) "widespread and well-known" weakness in the KYC processes for onboarding new clients; (ii) flaws in country and client AML risk ratings (including not rating Russia as "high risk" until late 2014); (iii) ineffective and understaffed anti-financial crime, AML and compliance units; and (iv) a decentralized AML organization, which caused confusion in policies, roles and responsibilities.[55]

Habib Bank Limited

(New consent order and $225 million penalty follows finding of continued weaknesses in the bank's risk management and compliance.)

On September 7, 2017, Habib Bank Limited ("HBL") and its New York branch[56] agreed to pay a $225 million fine as part of a consent order entered into with the DFS for failure to comply with New York AML laws and regulations.[57] In addition, HBL determined that it would wind down the New York branch's operation and surrender its license upon fulfillment of conditions outlined in a separate order.[58] Finally, HBL also agreed to expand the scope of a "lookback" review of transactions required under the 2015 consent order.[59]

The consent order states that it resulted from a 2016 DFS examination that noted weaknesses in HBL's risk management and compliance, as well as a failure to undertake remedial actions required by a consent order signed with the DFS in 2015. According to the most recent order, DFS found that HBL's AML program continued to suffer weaknesses in several areas: training, customer risk ratings, governance, OFAC and sanctions screening, independent testing and internal audit.[60]

Several of the deficiencies cited by the DFS pertained to transactions processed by HBL for one of its correspondent banking customers, the Al Rajhi Bank, which the DFS asserted had "reported links to al Qaeda."[61] The DFS also asserted that HBL had failed to identify that Al Rajhi Bank was processing transactions for Al Rajhi Bank affiliates, thus permitting unsafe "nested activity."[62]

Other deficiencies cited by the DFS include (i) allowing transactions to flow through the New York branch that potentially omitted information sufficient to properly screen for prohibited transactions or those otherwise involving sanctioned countries, and (ii) the improper use of a "good guy" list—a list of internally preapproved customers whose transactions were processed without screening.[63]

---

53 Similarly, the FCA noted that its fine included a 30% discount because the bank agreed to settle at an early stage of its investigation. *See* Press Release, FCA, FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings (Jan. 31, 2017), *available* here.
54 *Id.* at 9-13.
55 *Id.* at 13-17.
56 Debevoise & Plimpton serves as counsel to Habib Bank Limited and its New York Branch with respect to the DFS consent order.
57 *In the Matter* of *Habib Bank Limited*, Consent Order (N.Y. Bnk. Dept. Aug. 24, 2017), *available* here.
58 *Id.* at 54.
59 *Id.* at 51.
60 *Id.* at 5.
61 *Id.* at 6. *See*, *e.g.*, United States Senate Permanent Subcommittee on Investigations, Staff Report, U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History (July 17, 2012).
62 *Id.*
63 *Id.*

Nonghyup Bank

(Persistent AML deficiencies lead to a relatively low financial penalty of $11 million.)

On December 21, 2017, Nonghyup Bank ("Nonghyup") and its New York branch agreed to pay an $11 million fine as part of a consent order entered into with the DFS for failure to comply with AML laws and regulations.[64] Nonghyup, one of the largest commercial lenders in Korea, opened up its New York branch in 2013 and by 2017 held approximately $460 million in assets.[65] From 2014 through 2016, the DFS found the branch to have significant deficiencies in several areas, including BSA/AML risk assessments, customer due diligence and suspicious activity reporting, and to employ personnel lacking sufficient AML expertise.[66]

This enforcement action is notable for its relatively low fine of $11 million compared to all other AML penalties levied by the DFS in 2016 and 2017, which averaged $256 million.

DFS Opposition to the OCC's Proposal to Create a New National Bank Charter for "FinTech" Companies

On January 17, 2017, Superintendent Vullo submitted a letter in opposition to an OCC proposal to create a new national bank charter for financial technology ("FinTech") companies.[67] The Superintendent's comments followed the publication in December 2016 by the OCC of a white paper proposing the creation of the new chart type. Among other reasons cited for DFS's opposition, the Superintendent argued that state regulators like the DFS are better equipped than the OCC to oversee cash-intensive, nonbank financial service companies, which requires strict oversight and enforcement of anti-money laundering, consumer identification and transaction monitoring statutes and regulations.

As if to prove its ability to effectively regulate FinTech companies, that same day the DFS announced that it had approved the application of Coinbase, Inc. for a virtual currency and money transmitter license, following a comprehensive review of Coinbase's applications and policies, including the company's AML policy.[68] The DFS announcement added that, as of that date, it had approved a total of five firms for virtual currency charters or licenses, while denying applications from other firms that did not meet its standards.

On May 12, 2017, after the OCC had announced its intention to proceed with the new national bank charter for FinTech companies,[69] DFS Superintendent Maria Vullo sued the OCC in federal district

64 *In the Matter* of *Nonghyup Bank*, Consent Order (NYDFS, December 21, 2017), *available* here.
65 *Id.* at 3.
66 *Id.* at 9.
67 NYDFS, Letter to the OCC, Re: Exploring Special Purpose National Bank Charters for Fintech Companies (Jan. 17, 2017), *available* here.
68 Press Release, NYDFS, DFS Grants Virtual Currency License to Coinbase, Inc. (Jan. 17, 2017), *available* here.
69 In March 2017, the OCC proceeded to issue a draft supplement to its licensing manual setting forth proposed key components of the application and approval process in the proposed charter. In a separate release on the same day, the OCC addressed comment letters it had received on the charter, some of which were highly critical of the proposal on both policy and practical grounds. *See* Client Update, Debevoise & Plimpton LLP, OCC Proposes Chartering Process for FinTech Firms (Mar. 29, 2017), *available* here, for a review of the OCC's licensing plan.

Continued on page 15

DFS Opposition to the OCC's Proposal to Create a New National Bank Charter for "FinTech" Companies (Continued)

court in New York challenging the plan, citing the OCC's lack of authority to proceed[70] and reiterating that state regulators are better equipped to regulate such companies.[71]

On December 12, 2017, the court dismissed the case, ruling that the case was not yet ripe and the DFS Superintendent had not yet suffered injury by the actions of the OCC, because the OCC had not yet reached a final decision regarding the issuance of the national bank charter for FinTech companies.[72]

DFS Opposes MUFG's Switch to an OCC National Charter

On November 7, 2017, Mitsubishi UFJ Financial Group Inc. ("MUFG") received approval from the OCC to convert state-supervised branches into federally regulated ones. [73] MUFG had been regulated by state regulators, including DFS, which had fined the bank twice: $250 million in 2013, for allegedly stripping information from wire transfers involving sanctioned countries,[74] and $315 million in 2014, for allegedly causing the consultancy firm PricewaterhouseCoopers to alter a report submitted to the DFS.[75]

In response to the OCC's approval of MUFG's conversion to a national charter, the DFS reportedly issued a letter accusing the OCC of precipitous action, taken with a week's notice and "without the full factual record of [the bank's] compliance deficiencies," noting that the DFS was about to downgrade MUFG's supervisory rating.[76]

The New York Times cited the OCC's approval of MUFG's license as an example that the agency has reversed its previous inclination as one of the toughest financial regulators in the country.[77]

On November 8, 2017, MUFG sued the DFS to stop the Department's effort to continue to supervise the bank.[78] The case is pending.

---

70 Complaint, *Vullo v. Office of the Comptroller of the Currency*, 2017 WL 2115444 (S.D.N.Y. May 12, 2017) (Trial Pleading), *available* here.

71 NYDFS, Statement by Superintendent Maria T. Vullo on the DFS lawsuit challenging the OCC's unauthorized decision to grant special purpose national bank charters to undefined Fintech companies (May 12, 2017), *available* here.

72 *Vullo v. Office of the Comptroller of the Currency*, 17 Civ. 3574 (S.D.N.Y. Dec. 12, 2017), *available* here.

73 *See*, *generally*, Olivia Oran, "Exclusive: Japan's MUFG Gets Nod to Bring U.S. State Branches Under Federal Regulation," Reuters, Nov. 7, 2017, *available* here.

74 *In the Matter of Bank of Tokyo-Mitsubishi UFJ*, Consent Order (N.Y. Bnk .Dept. June 19, 2013), *available* here.

75 *In the Matter of Bank of Tokyo-Mitsubishi UFJ*, Consent Order (N.Y. Bnk. Dept. Nov. 18, 2014), *available* here.

76 *See* Ryan Tracy, "Switching U.S. Regulators Upends Probe into Japan's Biggest Bank," Wall St. J., Nov. 15, 2017, *available* here (with link for DFS letter to OCC).

77 Ben Protess, "Under Trump, Banking Watchdog Trades Its Bite for a Tamer Stance," N.Y. Times, Nov. 15, 2017, *available* here.

78 Complaint, *Bank of Tokyo-Mitsubishi UFJ v. Vullo*, No. 1:17-cv-08691 (S.D.N.Y. Nov. 8, 2017) (Trial Pleading); *See also,* Olivia Oran, "Japan's MUFG sues New York regulator over bank's oversight shift," Reuters, Nov. 8, 2014, *available* here.

Office of the Comptroller of the Currency

Citibank, N.A.

(The OCC announces a substantial civil money penalty against Citibank relating to failure to comply with prior consent order.)

On December 27, 2017, Citibank, N.A. ("Citibank") agreed to pay a $70 million fine as part of a consent order with the Office of the Comptroller of the Currency ("OCC") for failing to comply with the agency's 2012 consent order related to BSA and AML deficiencies.[79] In its 2012 order, the OCC cited the bank for BSA violations, deficiencies in its compliance program, failing to file suspicious activity reports, and weaknesses in controls related to correspondent banking.[80]

79 *In the Matter of Citibank, N.A.*, Consent Order for a Civil Money Penalty (OCC. December 27, 2017), *available* here.
80 *In the Matter of Citibank, N.A.*, Consent Order (OCC April 5, 2012), *available* here.

Federal Reserve Board

Deutsche Bank II

(Unsafe and unsound practices at the firm's domestic banking operations; $41 million penalty)

On May 30, 2017, the Federal Reserve Board ("FRB") announced it would impose a $41 million penalty and enter into a consent order with Deutsche Bank AG for AML deficiencies.[81] According to the consent order, this enforcement action was a result of a recent FRB examination of the BSA/AML program of Deutsche Bank Trust Company Americas and Deutsche Bank's New York branch—the same entities that were the subject of the enforcement actions by the DFS and FCA several months earlier.

According to the FRB, its exam identified significant deficiencies in Deutsche Bank's transaction monitoring capabilities that prevented the bank from properly assessing BSA/AML risk between 2011 and 2015 for billions of dollars in potentially suspicious transactions processed for certain affiliates in Europe.[82] While this action appears to be based on the same activity covered by the DFS enforcement action brought in January 2017 (*See* "Deutsche Bank I," *above*), the FRB action makes no reference to the earlier stated action.

81 Press Release, Federal Reserve Board of Governors, Federal Reserve Board Announces $41 Million Penalty and Consent Cease and Desist Order Against Deutsche Bank AG (May 30, 2017), *available* here.
82 *In the Matter of Deutsche Bank AG*, Order to Cease and Desist and Order of Assessment of a Civil Money Penalty Issued upon Consent (F.R.B. May 26, 2017), *available* here.

U.S. Securities and Exchange Commission

John Telfer (Meyers Associates L.P.)

(SEC settlement bars former AML officer for gatekeeper failures; $10,000 penalty for the AML officer and a $200,000 penalty for the firm.)

On June 12, 2017, John D. Telfer, the former chief compliance officer and AML officer of Meyers Associates, L.P., a registered broker-dealer, agreed to a CMP of $10,000 and a securities industry bar to settle charges brought by the SEC in a proceeding related to what the SEC defined as "gatekeeper failures."[83] On July 28, 2017, Meyers Associates, L.P. similarly agreed to pay a $200,000 civil penalty and retain an independent compliance consultant to review and monitor its AML program.[84] As the firm's AML officer, Mr. Telfer was "personally responsible for ensuring the firm's compliance with SAR reporting requirements," the SEC said, but failed to fulfill these responsibilities, even though certain red flags were brought directly to his attention through, for example, notifications from Meyers Associates' clearing firm.[85]

The SEC instituted proceedings against Mr. Telfer and his former employer Meyers Associates (now known as Windsor Street Capital, L.P.) on January 25, 2017. According to the SEC's settled order as to Mr. Telfer, [86] Meyers Associates failed to file SARs for approximately $24.8 million in suspicious transactions that the SEC said were marked by numerous red flags suggesting that certain customers of the firm were involved in fraudulent "pump and dump" schemes.[87]

According to the SEC, these red flags included (i) past securities fraud convictions or settlements by customers or related parties; (ii) inconsistencies between the customers' representations and documentation submitted to the firm; (iii) customers acquiring shares at very large discounts; (iv) signs that documents submitted were not authentic; (v) recent changes in the issuers' business model, including new business ventures relating to illegal industries, such as marijuana production and distribution; (vi) trading into sudden spikes in price and volume; and (vii) coordinated deposits and trading between one or more customers' accounts.

Alpine Securities Corporation

(SEC files complaint for insufficient SAR narratives.)

On June 5, 2017, the SEC charged Alpine Securities Corporation ("Alpine") with securities law violations for both failing to file SARs for stock transactions that it flagged as suspicious and for frequently failing to articulate the basis of its suspicions when the firm did file a SAR.[88] The SEC's action, which is pending, seeks permanent injunctions against Alpine enjoining it from engaging in the practices alleged in the complaint, as well as CMPs.

Alpine is a self-clearing broker-dealer based in Salt Lake City whose business mostly involves clearing microcap stock transactions for other firms.[89] According to the complaint, between May 2011 and

83 Administrative Summary, U.S. Securities and Exchange Commission, SEC Settlement Bars Former Anti-Money Laundering Officer for Gatekeeper Failures (June 12, 2017), *available* here.
84 Administrative Summary, U.S. Securities and Exchange Commission, SEC Settlement Limits Activities of Broker-Dealer that Engaged in Gatekeeper Failures (July 28, 2017), *available* here.
85 *Id.* at 2-3.
86 *In the Matter of Windsor Street Capital*, Corrected Order Making Findings and Imposing Remedial Sanctions and a Cease-and-Desist Order (S.E.C. Jan. 25, 2017), *available* here.
87 The SEC had previously charged several individuals in connection with a related "pump and dump" scheme. *See* Complaint, *S.E.C. v. Barton*, 2017 WL 361426 (E.D.N.Y. 2017) (Trial Pleading), *available* here.
88 Complaint, *S.E.C. v. Alpine Securities Corp.*, 2017 WL 2439016 (S.D.N.Y. 2017) (Trial Pleading), *available* here.
89 *Id.* at 5.

Continued on page 18

Alpine Securities Corporation (Continued)

December 2015, most of Alpine's clearing business came from Scottsdale Capital Advisors Corp ("Scottsdale"),[90] which shared common ownership with Alpine.[91] While Alpine filed thousands of SARs per year—more than any other individual broker-dealer, according to the complaint—it seldom closed Scottsdale-related accounts or refused to clear trades generated by such accounts.[92]

Instead, as alleged by the SEC and during the period of time covered by its complaint, Alpine systematically omitted from at least 1,950 SARs material "red-flag" details of which the firm was aware filed SARs only on the deposit of stock in approximately 1,900 instances in which the stock was subsequently liquidated (but failed to file on subsequent related transactions, such as the liquidation) and filed at least 250 SARs late.[93]

Wells Fargo Advisors LLC

(Failure to file SARs on continuing suspicious activity; $3.5 million penalty.)

On November 13, 2017, Wells Fargo Advisors, LLC, a registered broker-dealer located in St. Louis, Missouri, agreed to pay a civil penalty of $3.5 million to settle charges by the Securities and Exchange Commission ("SEC") that it failed to timely file a number of SARs between approximately March 2012 and June 2013.[94] According to the SEC's order, most of these failures related to continuing suspicious activity occurring in accounts held at Wells Fargo Advisors' U.S. branch offices that focused on international customers.[95] In addition to the payment of the civil penalty of $3.5 million, Wells Fargo Advisors consented to a cease-and-desist order and a censure, and voluntarily agreed to review and update its policies and procedures and develop and conduct additional training.

To help detect potential violations of the securities laws and other money laundering violations, the BSA requires broker-dealers to file SARs to report suspicious transactions that occur through their firms.[96] The BSA and FinCEN require the filing of a SAR within 30 days after a broker-dealer determines the activity is suspicious.[97] For SARs identifying continuing activity of a previously-filed SAR, FinCEN provides administrative relief which allows broker-dealers to file SARs for continuing activity within 120 days after the previously related SARs filing.[98]

According to the SEC's order, starting in March 2012, new managers within Wells Fargo Advisors' AML program created confusion by telling the firm's SAR investigators that (i) they were filing too many SARs, (ii) continuing-activity SAR reviews were not a regulatory requirement, (iii) they were to take steps to eliminate further continuing activity reviews and (iv) filing a SAR required "proof" of illegal activity.[99] These statements allegedly created an environment in which the SARs investigators experienced difficulty in recommending and filing SARs, especially continuing-activity SARs. SAR filings dropped by 60% during this period,[100] and Wells Fargo Advisors failed to timely file at least 50 SARs, 45 of which related to continuing activity.[101]

---

90 *Id.* at 7.
91 *Id.* at 5-6.
92 *Id.* at 8.
93 *Id.* at 3.
94 Administrative Summary, U.S. Securities and Exchange Commission, SEC Charges Wells Fargo Advisors with Failing to Comply with Anti-Money Laundering Laws (November 13, 2017), *available* here.
95 *In the Matter of Wells Fargo Advisors*, Order Instituting Administrative and Cease-and-Desist Proceedings. Release No. 34-82054, 2017 WL 5248280 (S.E.C. Nov. 13, 2017), *available* here.
96 *See* 31 CFR 1023.320.
97 *See* 31 CFR 1023.320(b)(3).
98 *See* FinCEN, Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report, Question #16, *available* here.
99 *Wells Fargo Advisors*, 2017 WL 5248280, at 4.
100 *Id.*
101 *Id.* at 5.

International

Deutsche Bank AG

(UK Financial Conduct Authority imposes record financial penalty for failure to report Russian "mirror-trading" scheme.)

As discussed above,[102] in connection with an investigation and consent order issued by the New York State Department of Financial Services ("DFS"), in January 2017, the UK FCA fined Deutsche Bank $204 million (£163,076,224) for failing to maintain an adequate AML control framework during the period between January 2012 and December 2015. According to the FCA, the fine was the largest financial penalty for AML violations ever imposed by that agency or its predecessor, the Financial Services Authority. [103]

Tabcorp

(AUSTRAC[104] announces Australia's highest-ever corporate civil penalty; $45 million.)

On March 16, 2017, the Federal Court of Australia ordered a $45 million civil penalty against Tabcorp, a gambling and entertainment company, for non-compliance with Australia's Anti-Money Laundering and Counter-Terrorism Financing Act 2006 ("AML/CTF Act").[105] The penalty was the country's highest-ever corporate civil penalty, according to Australia's financial intelligence agency, AUSTRAC, and resulted from Tabcorp's contravention of the AML/CTF Act over a period of more than five years by failing to timely report suspicious matters and for otherwise failing to have a compliant AML/CTF program.[106]

Commonwealth Bank of Australia

("Serious and systemic" AML failures in connection with rollout of new technology.)

On August 3, 2017, AUSTRAC initiated civil penalty proceedings against the Commonwealth Bank of Australia ("CBA") alleging over 53,700 contraventions of the AML/CTF Act.[107] In responding to the 580-page statement of claim filed by AUSTRAC, CBA disclosed that it will take a significant amount of time to file a defense in the matter,[108] but noted that while each offense carries a penalty of up to $18 million, the alleged contraventions could be considered to emanate from a single systems error. [109]

---

102 *See* "Deutsche Bank I," *above*.
103 Press Release, FCA, FCA fines Deutsche Bank £163 Million for Serious Anti-Money Laundering Control Failings (Jan. 31, 2017), *available* here.
104 AUSTRAC (the "Australian Transaction Reports and Analysis Centre") is Australia's financial intelligence agency with regulatory responsibility for anti-money laundering and counter-terrorism financing.
105 Press Release, AUSTRAC, Record $45 million civil penalty ordered against Tabcorp (Mar. 16, 2017), *available* here.
106 *Id.* The AML/CTF Act requires a reporting entity, *inter alia*, to submit Suspicious Matter Reports ("SMRs") to AUSTRAC when the entity forms a suspicion while dealing with a customer on a matter that may be related to an offense, tax evasion or proceeds of crime. *See* AUSTRAC Compliance Guide, AML/CTF Reporting Obligations, *available* here.
107 Press Release, AUSTRAC, AUSTRAC seeks civil penalty orders against CBA (Aug. 3, 2017), *available* here.
108 *See, e.g.*, Peter Ryan, "CBA Will Take Months to Answer Money Laundering Allegations," ABC News, Sept. 4, 2017, *available* here.
109 Press Release, Commonwealth Bank of Australia, Commonwealth Bank provides ASX update on AUSTRAC (Aug. 7, 2017), *available* here.

Continued on page 20

Commonwealth Bank of Australia (Continued)

The failures alleged by AUSTRAC pertain to CBA's 2012 rollout of Intelligent Deposit Machines ("IDMs"), a type of ATM that accepts deposits of cash and checks, which are automatically counted and credited instantly to the designated recipient's account. The funds are then available for immediate transfer to other accounts both domestically and internationally.

The IDMs allegedly permitted the deposit of up to $20,000 per transaction, with no limit on the number of transactions per day. IDMs also allegedly facilitated anonymous cash deposits, according to AUSTRAC. While deposits could only be made into CBA accounts, a bank card from any financial institution could be used to initiate a deposit and if the card entered into the machine was not issued by CBA, the cardholder's details were not known to CBA. In the months of May and June 2016 alone, over $1 billion in cash was allegedly deposited each month through IDMs.[110] According to AUSTRAC, at least four money laundering syndicates exploited IDMs to launder criminal proceeds.[111]

"Serious and systemic" AML failures alleged by AUSTRAC, include: failure to conduct risk assessments of the IDMs before their rollout, failure to monitor transactions on 778,370 accounts, failure to timely file 53,506 threshold transaction reports ("TTRs") for cash transactions of $10,000 or more and failure to timely report suspicious transactions totaling over $77 million.[112]

HSBC Private Bank

(French tax and money laundering investigation ends in first use of law modeled on U.S. deferred prosecution agreements; $352 million penalty.)

On November 14, 2017, HSBC agreed to pay EUR 300 million ($352 million) to settle a long-standing investigation by French prosecutors related to tax offenses involving HSBC Private Bank (Suisse) SA.[113] According to media reports, the investigation began in 2014 and included a review of whether the bank was complicit in laundering the proceeds of tax evasion.[114]

The agreement between the bank and the National Financial Prosecutor is the first such agreement entered into under the Judicial Convention of Public Interest since the procedural mechanism was first introduced in 2016.[115]

Long criticized for ineffective enforcement of their anti-corruption legislation, in December 2016, France passed the long-pending "Law Regarding Transparency, the Fight Against Corruption and the Modernization of Economic Life,"[116] known as the Loi Sapin II. The law provides for significant changes in the current French anti-corruption legal and regulatory administrative structure.

One new procedure, first utilized in the HSBC matter and known as the Judicial Convention in the Public Interest or "(JCPI)," permits a negotiated outcome for legal entities—but not individuals—that avoids a criminal conviction for offenses related to public and private corruption, whether domestic or foreign, as well as of laundering the proceeds of tax crimes.[117]

---

110 Concise Statement, *CEO of AUSTRAC v. Commonwealth Bank of Australia Limited*, (Aug. 3, 2017), at 1, *available* here.
111 *Id.* at 3-4.
112 Press Release, Commonwealth Bank of Australia, *supra* note 96, at 1.
113 Press Release, HSBC Private Banking, HSBC settles French legacy investigation (Nov. 14, 2017), *available* here.
114 *See, e.g.*, Brian Blackstone, "HSBC to Pay $352 Million to Resolve French Probe," Wall St. J., Nov. 14, 2017, *available* here.
115 Press Release, HSBC Private Banking, *supra* note 100.
116 Loi N°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, Journal Officiel (Dec. 10, 2016) [hereinafter *Loi Sapin II*], *available* here; *see also*, FCPA Update, Debevoise & Plimpton LLP, The Year 2016 in Anti-Corruption Enforcement: Record-Breaking Activity and Many Open Questions (Jan. 8, 2017), *available* here.
117 Loi Sapin II, at art. 22.

Regulations Based on European Union's Fourth Anti-Money Laundering Directive Come into Full Force

(Member states were required to fully implement the Directive by June 26, 2017.)

The EU's Fourth Anti-Money Laundering Directive, enacted in May 2015, brings forth many changes to European anti-money laundering regulations.[118] European states had until June 26, 2017 to enact the changes put forth in the Directive.

The changes, which largely implement recommendations from the Financial Action Task Force ("FATF"), represent the latest effort by the continent to make it more difficult for individuals to cover up money laundering activity. Among other changes, the Directive increased the transparency requirements surrounding beneficial ownership by requiring companies to maintain detailed records evidencing such ownership and making them available on a central register.[119] The Directive also removed the distinction between "external" and "internal" politically exposed persons ("PEPs"), meaning that a higher degree of caution and diligence is required even when dealing with domestic PEPs. The Directive also introduced increased focus on senior management, who now must ensure that they are adequately trained and prepared to meet the Directive's requirements.

---

118 *See* Directive 2015/849, of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, 2015 O.J. (L 141), *available* here.

119 *Id*. For a full review of the Directive's requirements and its recent implementation in the United Kingdom in particular, *see* Client Update, Debevoise & Plimpton LLP, Fourth Anti-Money Laundering Directive Comes Into Force (Aug. 3, 2015), *available* here; Client Update, Debevoise & Plimpton LLP, UK Implements New Anti-Money Laundering Rules (June 27, 2017), *available* here.

Summary Chart of 2017 AML Enforcement Actions

Entity	Date	Agency	AML Issue	Monetary Penalty	Other Measures
Western Union	19-Jan-2017	DOJ, FinCEN, FDIC	AML program, MSB agent oversight, wire fraud	$586 million	Independent compliance auditor
Deutsche Bank AG	30-Jan-2017	DFS,[120] FCA2 [121]	AML program, SAR reporting	$629 million	None
Merchants Bank of California, N.A.	27-Feb-2017	FinCEN, OCC	AML program, SAR reporting, BSA officer independence, insider misconduct	$7 million	None
Tabcorp	16-Mar-2017	AUSTRAC[122]	AML/CFT program, SAR reporting	$45 million	None
Banamex USA (Citigroup)	18-May-2017	DOJ	Individual liability, AML program, SAR reporting	$237.4 million	FDIC action: $190,000 in fines and employment bars for individuals
Thomas Haider (MoneyGram)	24-May-2017	FinCEN, DOJ	Individual liability, SAR reporting, MSB agent oversight	$250,000	Industry employment bar
Deutsche Bank AG	26-May-2017	FRB	AML program, safety and soundness	$41 million	None
Alpine Securities Corporation	5-Jun-2017	SEC	SAR reporting, securities clearing relationship	Case pending	Case pending
John Telfer (Meyers Associates, L.P.)	12-Jun-2017	SEC	Individual liability, AML program, SAR reporting	$10,000	Industry employment bar
BTC-E a/k/a Canton Business Corporation and Alexander Vinnik	27-Jul-2017	FinCEN, DOJ	Individual liability, virtual currency exchange	$110 million	Criminal indictment, $12 million individual fine
Meyers Associates, L.P.	28-Jul-2017	SEC	AML program, SAR reporting	$200,000	Independent consultant
Commonwealth Bank of Australia (CBA)	3-Aug-2017	AUSTRAC	AML/CTF program, risk assessment, transaction monitoring, SAR reporting	Case pending	Case pending

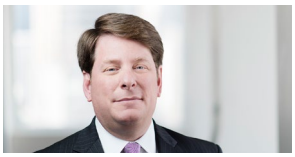
120 The New York State Department of Financial Services.
121 The UK Financial Conduct Authority.
122 The Australian Transaction Reports and Analysis Centre.

Continued on page 23

Summary Chart of 2017 AML Enforcement Actions (Continued)

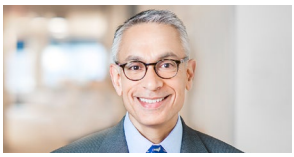
Entity	Date	Agency	AML Issue	Monetary Penalty	Other Measures
Habib Bank Limited and Habib Bank Limited, New York Branch	24-Aug-2017	DFS	OFAC screening, AML program, risk management	$225 million	Independent consultant, transaction lookback
Lone Star National Bank	1-Nov-2017	FinCEN	Correspondent banking due diligence	$2 million	None
Wells Fargo	13-Nov-2017	SEC	SAR reporting on continuing activity	$3.5 million	None
HSBC	14-Nov-2017	France/National Financial Prosecutor	Aggravated laundering of tax fraud proceeds	$352 million	First use of French DPA
Artichoke Joe's Casino	17-Nov-2017	FinCEN	AML program, SAR reporting	$8 million	None
Nonghyup Bank, and Nonghyup Bank New York Branch	21-Dec-2017	DFS	AML program	$11 million	None
Citibank, N.A.	27-Dec-2017	OCC	AML program, correspondent banking controls, SAR reporting	$70 million	None

Contributors



Matthew L. Biben
Partner
New York
+1 212 909 6606
mlbiben@debevoise.com

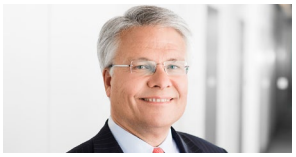
Helen V. Cantwell
Partner
New York
+1 212 909 6312
hcantwell@debevoise.com



Satish M. Kini
Partner
Washington, D.C.
+1 202 383 8190
smkini@debevoise.com

David A. O'Neil
Partner
Washington, D.C.
+1 202 383 8040
daoneil@debevoise.com

David Sarratt
Partner
New York
+1 212 909 6864
dsarratt@debevoise.com



Bruce Yannett
Partner
New York
+1 212 909 6495
beyannett@debevoise.com

Zila Acosta-Grimes
Associate
New York
+1 212 909 6513
zracosta@debevoise.com

Robert T. Dura
Associate
Washington, D.C.
+1 202 383 8247
rdura@debevoise.com

Neal S. Shecter
Associate
New York
+1 212 909 6374
nsshechter@debevoise.com