International Anti-Money Laundering

Harry Dixon
Nicole S. Healy
Albert Janet
Jo Ritcey-Donohue
International Anti-money Laundering Committee

Harry Dixon, Nicole S. Healy, Albert Janet, and Jo Ritcey-Donohue*

I. Introduction

In 2018, the European Union significantly expanded and revised its anti-money laundering/counter terrorist finance (AML/CFT) directives. This article discusses those revisions, which are intended to provide better coordination among EU AML/CFT efforts and to address new threats, including those related to cryptocurrencies. This year-in-review update also addresses the 2018 Basel AML Index results, which annually ranks countries based on their AML/CFT risks.

Additionally, because actions in the U.S. have international implications, this article discusses certain developments in U.S. AML/CFT enforcement. The Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) continued its efforts to prevent misuse of the financial system by adopting a new rule requiring disclosure of beneficial ownership of accounts at covered financial institutions.1 FinCEN also extended and expanded the existing Geographic Targeting Orders (GTOs) requiring title insurers to identify all beneficial owners holding a twenty-five percent or greater interest in real estate purchased in whole or in part in cash, cash substitutes such as cashiers’ checks, or virtual currency.2 The expansion applies to residential property in twelve major metropolitan areas, at a reduced singular threshold of $300,000.3 Additionally, FinCEN cooperated with other U.S. agencies to target overlapping money laundering risks with

---

* Contributing authors: Harry Dixon, Taylor English Duma LLP (Atlanta, GA); Nicole S. Healy, Ropers Majeski Kohn & Bentley PC (Redwood City, CA); Albert Janet, Heres (Paris, France); Jo Ritcey-Donohue, JRD Law PLLC (Washington, DC). Mr. Dixon, Ms. Healy and Ms. Ritcey-Donohue served as editors of this article.


3. Id. at 1–2.

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW
related cross-border risks. Specifically, they focused on economic sanctions targeting Iran and corrupt funds from senior political officials.

A. THE EUROPEAN UNION’S FIFTH AND SIXTH ANTI-MONEY LAUNDERING DIRECTIVES

Money laundering is a key driver of criminal behavior. Consequently, it has been a major area of concern for the European Union for the past twenty years. With the advent of the digital age, it is easier to escape the oversight of regulators through the use of prepaid payment cards, PayPal accounts, cryptocurrencies, or mobile phone payments. The European Union has struggled to both keep pace with these new methods of money laundering and fill any regulatory and legislative loopholes.

In 2018, the European Union attempted to fill these regulatory gaps with EU Directive 2018/843, which was enacted on May 30, 2018; it amends EU Directive 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, known as the “Fifth Money Laundering Directive” (Fifth AML Directive). Soon after, the European Union enacted EU Directive 2018/1673 on October 23, 2018 (Sixth AML Directive), which was intended to combat money laundering by harmonizing the relevant criminal laws of Member States. These legislative efforts to increase coordination across the Member States further strengthens the legal framework to protect the European financial system from infiltration by dirty money or illicit proceeds.


Although not as extensive as the Fourth AML Directive of May 20, 2015, this upgrade introduces several significant changes to the European AML/CFT regime. The European Union enacted the Fifth AML Directive in response to the terrorist attacks perpetrated in Paris on November 13, 2015 and the Brussels bombings of March 22, 2016, which demonstrated the vulnerability of financial institutions to terrorist financing. In addition, the Fifth AML Directive was a reaction to the Panama Papers leaks of April 2016, which shed an embarrassing spotlight on offshore financial dealings. It comes into force just one year after the Fourth AML Directive was embedded into the national laws throughout the European Union and has five main functions.

First, the Fifth AML Directive is designed to enhance cooperation between the financial intelligence units (FIUs) from each Member State. The FIUs are central, national units responsible for receiving and analyzing information from private entities related to financial transactions that may be linked to money laundering and terrorist financing. Through the Fifth AML Directive, these FIUs will gain broader access to information through centralized bank and payment account registers or data retrieval systems.

Second, the Fifth AML Directive makes the registers of ultimate beneficial ownership (created under the Fourth AML Directive) publicly accessible for companies, which will help the general public identify the true

---


11. Fifth AML Directive, supra note 8, at 43 (“Recent terrorist attacks have brought to light emerging new trends, in particular regarding the way terrorist groups finance and conduct their operations.”).

12. See European Commission Statement STATEMENT/18/3429, Statement by First Vice-President Timmermans, Vice-President Dombrovskis and Commissioner Jourová on the Adoption by the European Parliament of the 5th Anti-Money Laundering Directive (Apr. 19, 2018) (“With its vote, the Parliament concludes an ambitious round of negotiations initiated two years ago. In July 2016, in the aftermath of the terrible terrorist attacks that struck the EU and the vast financial dealings uncovered by the ‘Panama Papers’, the Commission decided to take urgent counter-measures. The revised directive is part of that action plan.”).

13. See Fifth AML Directive, supra note 8, art. 1, at 68 (“Member States shall ensure that FIUs exchange, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by the FIU related to money laundering or terrorist financing and the natural or legal person involved . . . .”) (amending Fourth AML Directive, supra note 10, art. 53, at 106).

14. See What We Do, FIN. CRIMES ENF’T NETWORK, https://www.fincen.gov/what-we-do (last visited Feb. 15, 2019) (“FinCEN serves as the FIU for the United States and is one of more than 100 FIUs making up the Egmont Group . . . .”).

15. See Fifth AML Directive, supra note 8, at 47.
owners of firms operating in the European Union. This measure will put an end to the corrupt use of letterbox companies—known in the U.S. as shell companies—which are often used to launder money or hide assets. This measure will also require the granting of access to data on ultimate beneficial owners of trusts to authorities, as well as others demonstrating a legitimate interest. Access to the beneficial ownership registers at the EU level will be completed by 2021 to facilitate cooperation and exchange of information.

Third, the Fifth AML Directive significantly changes the crypto-market. Specifically, it will regulate the use of digital or virtual currencies (like Bitcoin, Ether, or Ripple), as well as limit the use of prepaid cards to transaction amounts of €150 or less for businesses and €50 for online transactions. To end the anonymity of virtual currencies, the measure will ensure that exchange platforms between virtual currencies and fiat currencies—as well as custodian wallet providers—are applying customer due diligence controls and are registered.

Fourth, the Fifth AML Directive limits business relationships or transactions involving third countries when companies identify significant weaknesses in these countries’ AML/CFT regimes. The European Union will have to establish safeguards and enhanced due diligence measures with regard to financial transactions to and from those countries to manage and mitigate the risks.

Finally, the Fifth AML Directive also instructs that professionals who provide services in connection with trading works of art—including those services carried out by art galleries and auction houses—must now identify their customers and report any suspicious activity when the value of the transaction (or a series of linked transactions) amounts to €10,000.00.

The Fifth AML Directive entered into force on July 9, 2018, and Member States have until January 10, 2020 to implement it into their national legislation. But in a note dated November 23, 2018, the Council of the

20. Id. art. 1, at 67 (replacing paragraph 1 of Fourth AML Directive, supra note 10, art. 47, at 104).
21. Id. art. 1, at 57–58 (inserting an article 18a into Fourth AML Directive, supra note 10).
22. Id.
24. Id. art. 4–5, at 73.
European Union invited Member States to transpose the Fifth AML Directive ahead of the 2020 deadline.\(^{25}\)


The Sixth AML Directive establishes baseline rules defining criminal offenses and sanctions related to money laundering to create uniformity among the Member States.\(^{26}\)

First, the Sixth AML Directive criminalizes money laundering when intentional and with the knowledge that the property was derived from criminal activity.\(^{27}\) It does not distinguish between property derived directly or indirectly from criminal activity.\(^{28}\)

To create continuity, the Sixth AML Directive compels Member States to ensure that money laundering is punishable by a maximum term of imprisonment of at least four years without prejudice to the individual nature of penalties and the circumstances in each individual case.\(^{29}\) Article 2 of the Sixth AML Directive includes twenty-two separate predicate offenses considered criminal activities throughout the European Union. For example, the directive includes insider trading and market manipulation, counterfeiting of currency, cybercrimes, environmental crimes, and illicit trafficking in narcotics drugs or arms.\(^{30}\)

The Sixth AML Directive also provides for tougher sanctions against corporate entities and legal persons, where the lack of supervision has facilitated the commission of an offense.\(^{31}\) These sanctions can include loss of entitlements to public benefits, exclusion from public funding or tender procedures, or judicial winding-up orders.\(^{32}\) This particular measure can ultimately lead to the permanent closure of establishments used to commit the offense.\(^{33}\) This new directive will have to be transposed into each Member States’ national law before December 3, 2020 through appropriate implementation measures.\(^{34}\)


\(^{26}\) Sixth AML Directive, *supra* note 9, at 23 (recital 5 of the directive).

\(^{27}\) *Id.* at 24 (recital 13 of the directive).

\(^{28}\) *Id.*

\(^{29}\) *Id.* (recital 14 of the directive); see also *id.* art. 5, at 28.

\(^{30}\) *Id.* art. 2, at 26–27.

\(^{31}\) *Id.* art. 7, at 28–29.

\(^{32}\) Sixth AML Directive, *supra* note 9, art. 8, at 29.

\(^{33}\) *Id.*

\(^{34}\) *Id.* art. 13, at 30.
B. The Basel AML Index 2018 Report

On October 9, 2018, the University of Basel’s Basel Institute on Governance released its seventh annual Basel Anti-Money Laundering Index (the Index). The Index is an independent annual ranking assessing the risk of both money-laundering and terrorist financing around the world. Scores are based on fourteen publicly available indicators, such as “anti-money laundering and countering the financing of terrorism (AML/CFT) frameworks, corruption risk, financial transparency and standards, and public transparency and accountability.”

The key features of the Index include an overview of 129 countries, ranked “according to their risk of money laundering and terrorist financing” as well as a “[r]esearch-led, composite index based on public sources and third-party assessments.” Finland is ranked as the lowest-risk country, ranked at 129, and Tajikistan is the highest-ranked country at Number one. The U.S. is ranked at eighty-two.

The Index’s methodology follows a process of independent research, data selection, weighting, and results verification. The main areas that impact a country’s score are:

1. Quality of AML/CFT framework (65%);
2. Corruption risk (10%);
3. Financial transparency and standards (15%);
4. Public transparency and accountability (5%); and
5. Political and legal risk (5%).

The Index puts money laundering and terrorist financing risks in context, noting they “continue to cripple economies, distort international finances and harm citizens around the globe,” with costs ranging from $500 billion to $1 trillion. Unfortunately, the Index reports “[m]ost countries are making little to no progress ending corruption and public transparency is showing signs of decline, with governments making less information available about how they manage public funds.” Furthermore, the Index reports that press

---

36. Id.
37. Id.
38. BASEL INST. ON GOVERNANCE, BASEL AML INDEX 2018 REPORT 2 (2018) [hereinafter INDEX 2018].
39. Id. at 3–5.
40. Id. at 4.
41. Id. at 11.
42. Id. at 12.
43. Id. at 2.
44. INDEX 2018, supra note 38, at 2 (footnote omitted).
freedom has declined slightly, despite the fact that multiple investigative reports such as the Panama Papers have been published in recent years.\footnote{45. Id.}

The Index reports a few negative key trends during the past year: (1) minor measurable progress countering money laundering; (2) program effectiveness lags behind technical compliance; (3) money laundering and terrorist financing are not isolated risks; and (4) no countries are rated as having zero risk in money laundering or terrorist financing.\footnote{46. Id. at 5-7.}

The Index has consistently measured slow progress in countries improving their risk scores.\footnote{47. Id. at 5.} Sixty-four percent of the countries on the Index can be loosely classified as significant risks for money laundering and terrorist financing activity.\footnote{48. Id.} Many countries have become bigger risks for money laundering and terrorism financing, with thirty-seven percent of countries faring worse on the Index than they did in 2012.\footnote{49. Id.}

Most countries have ineffective programs to combat these risks, even if the countries comply with those programs.\footnote{50. Index 2018, supra note 38, at 6.} Forty-seven percent of the countries have a low level of effectiveness in investigating and prosecuting money laundering offenses, and forty percent are not achieving outcomes from conducting asset forfeiture.\footnote{51. Id.}

The Index found that countries with a high risk of money laundering activity share some or all of the following characteristics: (1) weak rule of law; (2) low levels of transparency; (3) restrictions on press freedom; (4) inability to control the financial system due to lack of resources; (5) cash-based economies; and (6) high levels of smuggling and trafficking, whether in humans, drugs, wildlife, etc.\footnote{52. Id. at 7.} The interconnectedness of these factors meant that even where a country improved in some areas, deficiencies in other areas negated these improvements.\footnote{53. Id.}

According to the Index, even the countries with the lowest scores for money laundering risks still had areas of improvement.\footnote{54. Id.} For example, beneficial ownership issues and screening for politically exposed persons were present in every country.\footnote{55. Id. at 7-8.} Significantly, because money launderers constantly innovate, the task of effective money laundering compliance is never complete.\footnote{56. Index 2018, supra note 38, 7-8.} But the Index also noted that countries with low scores provide models for other countries.\footnote{57. Id. at 8.} Low risk countries like Finland, New Zealand, Sweden, and Israel all share: (1) strong legislation for anti-money laundering laws; (2) anti-money laundering and terrorist financing authorities that are effective; (3) the sharing of information between countries; (4) anti-money laundering and terrorist financing programs that are designed to be effective; (5) the protection of beneficial ownership information; and (6) the protection of politically exposed persons.
laundering and counter-terrorism financing; (2) competent authorities that can investigate and prosecute money laundering and terrorist financing offenses and sanction institutions for non-compliance; (3) comprehensive measures to ensure domestic and international cooperation; (4) high levels of press freedom allowing the press to actively uncover and report on stories of financial crime; and (5) highly-regulated financial sectors with few cash transactions and supervision by competent authorities.

On this year’s Index, countries with historically high scores witnessed improvement in their score. For those countries, two factors were consistently the cause. First, changes in the methodology underlying the Financial Secrecy Index—which measures the level of secrecy, a country’s offshore banking activity, and the size of a country’s financial center—altered some scores. Second, some countries were removed as “Jurisdictions of Primary Concern” from the U.S. State Department’s International Narcotics Control Strategy Report.

C. FinCEN’s New Customer Due Diligence (CDD) Rule for Financial Institutions

As of May 11, 2018, FinCEN, a bureau of the U.S. Treasury Department, requires “covered financial institutions” to obtain information concerning the beneficial ownership of newly-opened accounts held by “legal entity” customers. Not all entities otherwise subject to AML compliance requirements are included within this rule. Rather, the term “covered financial institution” means federally insured banks and credit unions, commercial banks, U.S. agencies or branches of foreign banks, savings associations, federally-regulated trust banks or companies, international or foreign banking corporations organized pursuant to 12 U.S.C. § 611 et seq.,

---

58. Id. at 8–9.
59. See id. at 9.
60. Id.
61. Id. at 10.
63. See 31 C.F.R. § 1010.230(b)(1) (2018). “Legal entity customer” is defined as “a corporation, limited liability company, or other entity that is created by the filing of a public document with a Secretary of State or similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account.” 31 C.F.R. § 1010.230(e)(1).
64. Note that entities that are otherwise defined as “financial institutions” for AML compliance purposes are not “covered financial institutions” under the new CDD Rule. For example, the following types of entities are not included within the rule: casinos, card clubs, and money services businesses, including providers of prepaid access and money transmitters. Compare 31 C.F.R. § 1010.100(e)(3)–(6), (ff)(4) (2018) (defining “financial institution”), with 31 C.F.R. § 1010.605(c) (2018) (defining “covered financial institution”), and 31 C.F.R. § 1010.230(f) (“For the purpose of this section, covered financial institution has the meaning set forth in § 1010.605(c)(1) of this chapter.”).
mutual funds, securities brokers and dealers, futures commission merchants, and introducing brokers in commodities.65

For purposes of the CDD Rule, “beneficial ownership” information means the identification of all persons owning twenty-five percent or more of a legal entity customer,66 and the identification of one control person.67 Some banks are reportedly setting lower reporting thresholds, as permitted by the rule.68 Moreover, while a single individual may occupy both categories, financial institutions must undertake both analyses.69

Where a “beneficial owner” holding a twenty-five percent or greater interest in a customer is itself a legal entity, including a trust, the rule provides for identification of one or more individuals holding that percentage ownership, except in the case of a trust. For trusts, the beneficial owner means the trustee; although, if the beneficial owner is an excluded entity, then no individual must be identified.70 Excluded entities include federally or state-regulated financial institutions; entities regulated by the Securities and Exchange Commission (SEC) or the Commodities Futures Trading Commission (CFTC); pooled investment vehicles operated by an excluded entity, bank or savings and loan holding companies; state-regulated insurance companies; foreign financial institutions “established in a

65. See 31 C.F.R. § 1010.605(e)(1).
66. Specifically, “[e]ach individual, if any, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns 25 percent or more of the equity interests of a legal entity customer.” See 31 C.F.R. § 1010.230(d)(1).
67. 31 C.F.R. § 1010.230(d)(2) (referring to “[a] single individual with significant responsibility to control, manage, or direct a legal entity customer, including: (i) [a]n executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or (ii) [a]ny other individual who regularly performs similar functions.”). 31 C.F.R. § 1010.230(d)(2).
68. 31 C.F.R. § 1010.230(d) note (“[a] covered financial institution may also identify additional individuals as part of its customer due diligence if it deems appropriate on the basis of risk.”).
69. In a note to paragraph (d) of section 1010.230, FinCEN cautions that the “number of individuals that satisfy the definition of ‘beneficial owner,’ and therefore must be identified and verified pursuant to this section, may vary.” 31 C.F.R. § 1010.230(d) note. Thus, given the twenty-five percent threshold under the ownership prong of paragraph (d)(1), “depending on the factual circumstances, up to four individuals may need to be identified.” Id. Under the control prong of paragraph (d)(2), “only one individual must be identified.” Id. FinCEN recognizes that a single individual may be identified under both prongs. Id. In addition, “[a] covered financial institution may also identify additional individuals as part of its customer due diligence if it deems appropriate on the basis of risk.” Id.
70. 31 C.F.R. § 1010.230(d)(3) (“If a trust owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, 25 percent or more of the equity interests of a legal entity customer, the beneficial owner for purposes of paragraph (d)(1) of this section shall mean the trustee. If an entity listed in paragraph (e)(2) of this section owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, 25 percent or more of the equity interests of a legal entity customer, no individual need be identified for purposes of paragraph (d)(1) of this section with respect to that entity’s interests.”).
jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution; and non-profit corporations. Essentially, where the entity is already subject to regulatory oversight, the CDD Rule does not require identification of individual beneficial owners with two exceptions. Specifically, both pooled investment vehicles operated or advised by financial institutions and not excluded under the CDD Rule, as well as state-chartered non-profit corporations, are subject to the control prong. Accordingly, the financial institution must identify a control person when opening a new account for one of these entities.

The term “new account” is defined as “each account opened at a covered financial institution by a legal entity customer on or after the applicability date.” That means not only accounts opened by new customers, but also any new accounts opened by, or new extensions of credit made to, a current customer after the effective date of the rule.

The CDD Rule requires financial institutions to “identify” the beneficial owner(s) of the account, “verify” their information, and maintain identification information for “five years after the date the account is closed,” as well as verification records “for five years after the record is made.” To satisfy the identification requirement, a covered financial institution may obtain a certification from the individual opening the account on behalf of the legal entity customer, or in some other form, so long as the individual certifies its accuracy.

---

71. 31 C.F.R. § 1010.230(c)(2)(xiv). This would appear to include financial institutions subject to the Fifth European Union Anti-Money Laundering Directive. See generally Fifth AML Directive, supra note 8.
72. For a complete list of the excluded entities, see 31 C.F.R. § 1010.230(c)(2)(i)-(xvi).
73. See 31 C.F.R. § 1010.230(c)(3).
74. 31 C.F.R. § 1010.230(g).
75. The term “account” is defined at 31 C.F.R. §§ 1020.100(a) (banks), 1023.100(a) (securities brokers or dealers), 1024.100(a) (mutual funds), and 1026.100(a) (futures commission merchants and introducing brokers in commodities). 31 C.F.R. § 1010.230(c). Each definition provides for a formal or contractual relationship to provide certain services. See, e.g., 31 C.F.R. § 1020.100(a)(1) (2018) (“Account means a formal banking relationship established to provide or engage in services, dealings, or other financial transactions including a deposit account, a transaction or asset account, a credit account, or other extension of credit. Account also includes a relationship established to provide a safety deposit box or other safekeeping services, or cash management, custodian, and trust services.”).
76. 31 C.F.R. § 1010.230(i).
77. 31 C.F.R. § 1010.230(b)(1). A covered financial institution may rely on CDD conducted by another financial institution, including an affiliate, concerning a legal entity customer: that is opening, or has opened, an account or has established a similar business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions, provided that: (1) such reliance is reasonable under the circumstances; (2) the other financial institution is subject to a rule implementing 31 U.S.C. § 5318(b) and is regulated by a Federal functional regulator; and (3) the other financial institution enters into a contract requiring it to certify annually to the covered financial institution that it has implemented its
requirement, the covered financial institution must “[v]erify the identity of each beneficial owner identified to the covered financial institution, according to risk-based procedures to the extent reasonable and practicable.” The rule provides a safe harbor for covered financial institutions. Specifically, they “may rely on information supplied by the legal entity customer regarding the identity of its beneficial owner or owners,” provided, however, that they have “no knowledge of facts that would reasonably call into question the reliability of such information.”

The CDD Rule exempts covered financial institutions from obtaining identification and verification information when they open certain kinds of accounts for legal entities. Such accounts are limited to providing point-of-sale credit products to purchase retail goods up to $50,000 or to finance postage, insurance premiums remitted to the provider or broker, or equipment leasing if remitted directly to the vendor or lessor. These limited exemptions are not available when the legal entity customer can make or receive payments to or from third parties or when cash refunds are available.

Although the CDD Rule appears reasonably comprehensive, some open questions remain. For example, an individual may hold indirect “ownership” of a legal entity through a “contract, arrangement, understanding, relationship, or otherwise . . . . But it is unclear how far these terms—in particular, “otherwise”—extend. Specifically, does “indirect” control exist on the basis of a put or a call option, right of first refusal, or other circumstance that gives an individual some potential future authority over a legal entity but not a present interest? In addition, the question remains whether FinCEN will expand the rule to cover other financial institutions, such as money services businesses, cryptocurrency platforms, casinos, and other entities not currently covered. The application of the CDD Rule in practice will bear watching.

---

31 C.F.R. § 1010.230(j), (l)-(3).
78. 31 C.F.R. § 1010.230(b)(2).
79. Id.
80. See 31 C.F.R. § 1010.230(b)(1).
82. 31 C.F.R. § 1010.230(b)(2).
83. 31 C.F.R. § 1010.230(d)(1).
84. The CDD Rule requires the aggregation of individual ownership interests, including indirect interests, linked or controlled “through any contract, arrangement, understanding, relationship or otherwise . . . .” 31 C.F.R. § 1010.230(d)(1).
D. AML COMPLIANCE AND ENFORCEMENT INCREASINGLY INTERSECT WITH OTHER CROSS-BORDER COMPLIANCE RISKS

During the past year, anti-money laundering laws and the government authorities that enforce them have explicitly overlapped with other cross-border risk and legal compliance areas—particularly economic sanctions and anti-bribery. This overlap has been most evident with respect to Iran, which for decades has been the target of U.S. and international sanctions and is increasingly the target of U.S. and international anti-money laundering risk mitigation actions. In addition, Iran—along with several other countries—has been identified as posing an elevated anti-money laundering risk precisely due to sanctions risks related to corruption and other human rights abuses. The U.S. and other governmental enforcement officials’ guidance and public notices identifying these cross-over risks between anti-money laundering and other cross-border compliance risks provide an indication of their expectations for corporate compliance internal controls.

1. AML Measures Targeting Iran

a. International

On October 19, 2018, the Financial Action Task Force (FATF), which is the international AML standard-setting body, gave Iran until February 2019 to implement previously recommended legal measures to counter money laundering or risk the imposition of restrictions on its global financial transactions. The impact of FATF actions will extend well beyond the U.S. and affect any financial market and commercial actors impacted by U.S. sanctions targeting Iran. Even countries that have maintained public ties with Tehran, such as Russia and China—which are both FATF members—would impose restrictions.

Only two countries, Iran and North Korea, are listed by FATF as countries of the highest concern for money laundering. Countries in this highest risk category are subject to FATF countermeasures, which can include prohibitions on financial transactions with the country creating a similar impact as the economic sanctions currently imposed by the U.S.

86. See FinCEN Advisory on Human Rights Abuses, supra note 4, at 2.
North Korea is currently subject to such countermeasures.\textsuperscript{90} Iran has avoided countermeasures for years by promising to undertake efforts to strengthen AML statutes and regulations and align them with internationally-accepted principles.\textsuperscript{91}

On June 24, 2016, FATF suspended the imposition of countermeasures on Iran for an initial period of twelve months based on Iran’s commitment to make improvements called for by the international body.\textsuperscript{92} Under the FATF suspension of countermeasures, which have been extended multiple times before the most recent extension until February 2018, Iran is required to take specific legal steps, including identifying and freezing terrorist assets targeted by U.N. Security Council sanctions and resolutions, and to adopt certain international norms, such as the Palermo and Terrorist Financing Conventions.\textsuperscript{93}

The FATF action plan for Iran expired in January 2018.\textsuperscript{94} Since that time, the Iranian government has reportedly been divided on whether to adopt the measures required by the FATF plan.\textsuperscript{95} Specifically, reports suggest hardliners in the Iranian government regime disfavor adopting the FATF requirements, which they see as a threat to Iran’s support for Hezbollah operating out of Lebanon, and Hamas, linked with the Palestinian Liberation Organization.\textsuperscript{96} Both Hezbollah and Hamas are considered international terrorist groups under U.S sanctions,\textsuperscript{97} but are not targeted by U.N. sanctions.\textsuperscript{98}
If Iran fails to meet the February deadline and FATF re-imposes countermeasures, banks and other financial institutions (FIs) around the globe will, at a minimum, impose heightened due diligence requirements for transactions involving Iran (many FIs in major jurisdictions do so already) and could eventually impose additional restrictions. For example, current FATF countermeasures on North Korea include financial sanctions, closures of North Korean banks in FATF countries, and terminated correspondent relationships with North Korean banks.99

b. United States

This past year, U.S. anti-money laundering legal authorities increased their publicly coordinated efforts with economic sanctions governmental authorities in order to target Iran. On October 11, 2018, FinCEN and the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) jointly issued notices regarding the money laundering threats posed by targets of U.S.-Iran sanctions.

The FinCEN notice reminded Financial Institutions (“FI”) about their U.S. correspondents’ obligations and warned against AML/CFT and U.S. economic sanctions risks.100 FinCEN noted Iran’s long-standing practice of using shell companies to evade detection by FIs when transferring funds that represent revenues from or support for activities targeted by U.S. economic sanctions, such as international terrorism, human rights abuses, and support for the Syrian Government.101 FinCEN’s stated aim was to highlight the Iranian government’s methods of exploiting “financial institutions worldwide” and identify “red flags” that FIs can use to detect such evasive tactics.102

FinCEN identified a number of red flags related to transfers from the personal accounts of senior officials of the Central Bank of Iran (CBI), the use of exchange houses and shell entities to transfer funds, commercial aviation trade in goods transactions, falsified shipping documentation, virtual currency transactions, and other suspicious transactions.103 FinCEN further requested that FIs include a special identifier—“Iran FIN-2018-A006”—in Suspicious Activity Reports (SARs) when related to Iranian sanctions or otherwise related to the new FinCEN Iran advisory.104

OFAC, which does not typically issue notices about FinCEN or other agency actions, issued a notice regarding FinCEN’s October 11, 2018 advisory on Iran. On October 16, 2018, OFAC designated a vast array of entities and individuals, including banks and investment companies, that “provided financial support” to a sanctioned entity, the Iranian

100. FinCEN Advisory on Iranian Regime’s Malign Activities, supra note 5, at 1.
101. Id.
102. Id.
103. Id. at 2.
104. Id. at 19.
Revolutionary Guard Corp.\textsuperscript{105} Subsequently, on November 20, 2018, OFAC issued an Advisory to the Maritime Petroleum Shipping Community, which among other things advised FIs and global companies to ensure compliance consistent with FATF AML/CFT standards and conduct enhanced due diligence to detect and deter against attempts to evade U.S. sanctions by Iranian and Syrian regime supporters.\textsuperscript{106}

2. U.S. AML Authorities Target Corruption

On June 12, 2018, FinCEN issued an Advisory detailing various anti-money laundering risks and red flags most commonly presented by corrupt government officials and politically exposed persons (PEPs).\textsuperscript{107} The FinCEN public notice highlighted U.S. economic sanctions laws and regulations that target corrupt PEPs and other human rights abusers, as well as the need for enhanced diligence to prevent those sanctions targets and other PEPs from abusing the U.S financial system.\textsuperscript{108} For instance, FinCEN noted that its sister agency in the U.S. Treasury Department, OFAC, targets corrupt PEPs under the Global Magnitsky Act of 2016, which authorizes the freezing of assets and other restrictions on individuals who engage in corrupt activity, cronyism, and other illegal activities.\textsuperscript{109} FinCEN identifies common means that such individuals employ to launder the proceeds of illicit activity and red flags to help detect and deter such laundering.\textsuperscript{110}

These country specific advisories are not new. FinCEN has previously issued country-specific advisories related to anti-money laundering risks posed by PEPs and targets of sanctions related to corruption. In September 2017, FinCEN issued such a notice with respect to Venezuela.\textsuperscript{111} In the latest notice in June 2018, FinCEN described three general methods commonly used to launder the proceeds of corruption through the U.S. financial system:

(1) Misappropriation of State Assets: Senior government officials may abuse their position by engaging in corruption or otherwise illegal activities, for their personal gain, and then launder those monies through shell companies and other businesses;
(2) Use of Shell Companies: Senior government officials use shell companies with no physical presence or operations “to obfuscate ownership and mask the true source of the proceeds of corruption”; and

(3) Corruption in the Real Estate Sector: Real estate transactions are particularly vulnerable to money laundering because they often involve limited transparency, multiple entities, and complexity.112

The Advisory provides fourteen red flags that should alert persons engaged in financial transactions with PEPs to take added precautions to protect against potential money laundering. These red flags include: (1) use of third parties when it appears to shield the identity of a PEP or his/her family member; (2) use of family members or close associates as legal owners; (3) declarations of information that are inconsistent with publicly available information, including availability of personal wealth or assets; and (4) a PEP or financial facilitator transferring funds among countries with which the PEP is not otherwise affiliated.113

112. FinCEN Advisory on Human Rights Abuses, supra note 5, 4–5.
113. Id. at 5–6.