INTERNATIONAL AML ENFORCEMENT IN 2017 EXPECTED TO TARGET CONSUMER-DUE-DILIGENCE PROGRAMS, GAMING ENTITIES, PREPAID CARDS, DIGITAL CURRENCIES, AND HIGH-RISK NESTED ACCOUNTS

Date: 29 November 2016

Government Enforcement Alert

By: Mark A. Rush, Judith Rinearson, Stefanie M. Lacy, Joseph A. Valenti

EXECUTIVE SUMMARY

Over the past two years, financial regulatory bodies in the United States and Europe have increasingly emphasized consumer due diligence ("CDD") by financial institutions as a means to combat money laundering and terrorist financing, especially with respect to "high risk" products. This trend is expected to continue in 2017.

Consistent with Financial Action Task Force ("FATF") guidance, the European Union and the United States have enacted regulations requiring certain financial institutions to implement some form of CDD on a variety of higher risk financial products. Chief among these are nested accounts (which include the individual consumer sub-accounts within a business customer's account) and accounts owned by shell corporations or straw owners. CDD best practices also encourage financial institutions to determine who ultimately benefits from a transaction and to assess their risk profile. Whether a financial institution's direct business customer is a payment processor, a prepaid card program manager, a digital currency platform, a gaming entity, a money-services business, or some other type of business that processes or holds money for its customers, it is increasingly clear that regulators expect such financial institutions to properly investigate and monitor both their direct business customers as well as the individuals or entities that ultimately use, control, or benefit from the transactions they facilitate.

For example, in the past, a bank could conduct due diligence only on its customer, digital currency provider Company A. Updated CDD expectations now push the bank to look beyond the digital currency provider Company A and conduct due diligence on the typical risk profile and transaction patterns of the individuals who ultimately use Company A (i.e. Company A's average customer), as well as the entities that own and control Company A (i.e., the "beneficial owners"). It is because of these expanded CDD requirements that many banks and financial institutions have opted not to do business with entities such as digital currency exchanges or providers; the compliance costs and risks arising from the increased CDD obligations have outweighed the potential benefits and revenues these customers can provide.

The CDD requirements place an increased responsibility on financial institutions to be cognizant of their customers and the ways in which a financial institution's products and services are being used. Some critics

argue that the regulations have grown to a point where financial institutions are involuntary "proxies for law enforcement"[1] because regulators now may take enforcement actions against them for failures to thoroughly investigate and report crime and suspicious activity passing through their services rather than just ensuring that their own direct actions are lawful. Whether or not that criticism is fair, the reality is that increasing compliance demands have been placed on financial institutions. Heading into 2017, financial institutions should thus review their anti-money-laundering ("AML") and CDD programs, update them as necessary, and retain independent, outside counsel or auditors to separately assess the efficiency of these controls.

CDD IS BECOMING INCREASINGLY IMPORTANT TO REGULATORS AROUND THE GLOBE

FATF Released New Guidance Involving CDD on Correspondent Accounts

The FATF — comprised of law enforcement organizations from a host of countries — has recognized the need to encourage global access to the financial system while at the same time aggressively detecting and preventing money laundering and financial crime. In October 2016, the FATF issued guidance on correspondent banking[2] to mitigate wholesale de-risking, "where financial institutions terminate or restrict business relationships with entire countries or classes of customer in order to avoid, rather than manage, risks."[3] "[D]e-risking may drive financial transactions into less/non-regulated channels, reducing transparency of financial flows and creating financial exclusion, thereby increasing exposure to money laundering and terrorist financing (ML/TF) risks."[4] De-risking also has the potential to violate civil rights in the United States if it results in the exclusion of communities from the financial system based on analysis skewed against them. To clarify that their prior guidance did not advocate complete de-risking, FATF explained that enhanced CDD struck a "middle ground" balance between encouraging global access to the financial system and combatting money laundering and financial crime. While requiring enhanced CDD can, like de-risking, increase compliance risks and may still lead to de-risking by many financial institutions, the FATF's hope is that it is possible to effectively and surgically prevent financial crime without preventing legitimate financial transactions on a wide scale or for a lawful group.

In its October 2016 guidance, the FATF made clear that it does "not require financial institutions to conduct customer due diligence on the customers of their customer (i.e., each individual customer)."[5] Nonetheless, the FATF and its member countries expect financial institutions to know — and perhaps audit — the compliance programs of its institutional customers and to understand and investigate the risk profiles, account usage, and related anomalies of institutional customers.[6]

In that vein, the FATF has defined "Money or Value Transfer Services ('MVTS')" as a CDD risk. MVTS are "financial services that involve the acceptance of cash, cheques, other monetary instruments or other means of stored value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs."[7] FATF has provided specific "additional guidance" for financial institutions with MVTS customers, which includes understanding whether the customer accounts belong to the customer for its own settlement purposes or are being used to facilitate underlying transfers or to hold customer assets.[8] Where the MVTS customer is separately servicing customers, the risk profile increases. By utilizing CDD, the FATF hopes that correspondent

banks can mitigate risks by focusing due-diligence efforts on whomever ultimately owns or benefits from the assets at issue.

The EU's Enactment of the Fourth and Fifth AML Directives

The Fourth and Fifth AML Directives are the broadest and most recent EU legislation addressing money laundering. The Fourth AML Directive, which has an effective date of June 26, 2017, is designed to "strengthen EU rules and to ensure their consistency with the global standards laid down in the international recommendations adopted by the Financial Action Task Force (FATF)."[9] The European Commission recently approved amendments proposed to the Fourth AML Directive, which are collectively referred to as the Fifth AML Directive, to address heightened concerns regarding terrorist financing — especially with respect to new "alternative financial systems"— explaining that:

> Recent terrorist attacks have brought to light emerging new trends, in particular regarding the way terrorist groups finance and conduct their operations. Certain modern technology services are becoming more and more popular as alternative financial systems and remain outside the scope of Union legislation or benefit from exemptions that may no longer be justified. In order to keep pace with evolving trends, further measures to improve the existing preventive framework should be taken.[10]

Among other things, these amendments in the Fifth AML Directive target anonymous prepaid cards by lowering the identification threshold from €250 to €150 and permitting EU member states, if they so choose, to prohibit merchants from accepting *any* payments made with anonymous prepaid cards. Thus, the purpose of the Fifth AML Directive amendments to the Fourth AML Directive is to improve access to data that identifies ultimate beneficial owners of relatively anonymous and transferrable assets, such as prepaid cards, digital currencies, and casino chips and to make it more difficult for these assets to be used for terrorist or criminal activity. While most of the Fifth AML Directive is also due to become effective on June 26, 2017, the provisions requiring financial-institution collection and law-enforcement access to beneficial-ownership information for the transferrable assets discussed above will become effective January 1, 2018.

- Taken together, some of the other key changes implemented by the Fourth and Fifth AML Directives include:
- Requiring the gambling sector to conduct CDD and report a broader range of transactions in certain cases;
- Requiring businesses receiving cash payments in excess of €10,000 to report such payments and implement relevant internal controls to ensure collection of data necessary to make these reports;
- Requiring financial institutions to conduct CDD on owners of trusts / legal entities, politically exposed persons, and individuals involved in high-risk situations such as trading with other banks sitting outside the EU;
- Prohibiting CDD enhancements and risk-mitigation efforts from being used in a discriminatory fashion;

- Requiring *all* "providers of exchange services between virtual currencies and fiat currencies" (not simply only those who did so "primarily and professionally") to implement effective AML controls and CDD programs; and
- Redefining "custodian wallet providers" as any "entity that provides services to safeguard private keys on behalf of their customers to hold, store and transfer virtual currencies," which in turn expands the number of technology and cybersecurity companies that now have AML reporting and internal-controls obligations.

FinCEN Imposed New CDD Requirements on Financial Institutions in the United States

In May 2016, the Financial Crimes Enforcement Network ("FinCEN") imposed new CDD requirements on financial institutions in the United States. The new regulations require financial institutions to conduct CDD on the beneficial owners of its institutional customers.[11] Similar to the FATF guidance, the FinCEN regulations do not require a financial institution to conduct due diligence on the individual customers of its institutional customer. However, the regulations do require financial institutions to conduct due diligence on the owners of institutional and legal-entity customers, such as corporations, trusts, and other entities. To the extent that these legal-entity customers fit within a specific industry or have customers of their own, the financial institution servicing these legal entities must assess their risk profile and monitor their activities to ensure that it is consistent with that profile. For instance, a traditional bank servicing a digital-currency provider is expected to know the average number of transactions made in that digital currency and recognize and report a dramatic and suspicious spike in such transactions through the provider's account at the bank. Although compliance with the new FinCEN regulations is not required until May 2018, FinCEN's imposition of CDD requirements further evidences the trend towards government scrutiny of CDD programs and high-risk nested accounts.[12]

KEY INDUSTRIES AT RISK

As technology grows, so does the risk. Newer technologies such as virtual currencies and prepaid gift cards pose higher risks for money laundering and financial crime, in part, because the ultimate consumer using these technologies is difficult to ascertain. Virtual currency poses additional regulatory difficulties, given that many businesses in the virtual currency space do not utilize banks, which cuts out third parties, and are not subject to any one jurisdiction's financial laws.

Evolving industries, such as online gaming services and online money remitters, are also at higher risk. These industries typically require the support of traditional financial institutions to survive and grow, but they may not currently use CDD on their institutional customers (as lower overhead costs and speedier transactions for online platforms are among their primary competitive business advantages). Potential AML risks for online services include "front men" that engage in transactions on behalf of a bad actor, the use of false or unverified identities, speedy cross-border transactions, and the service provider's ability to credit money to accounts other than the originator without the knowledge of the traditional financial institution facilitating the provider's transactions.

CROSS-BORDER COOPERATION BY GOVERNMENTS ON AML ISSUES IS INCREASING

Ongoing fallout from the investigations and prosecutions related to Liberty Reserve (a virtual currency market) has led to international AML cooperation, including extradition.[13] New directives from both the EU and FinCEN have moved the FATF guidance toward action, calling for increased cross-border cooperation and higher customer due-diligence standards — particularly on high-risk accounts.

In one 2016 case announced in September, a Chinese trading company charged by the U.S. Department of Justice ("DOJ") with laundering money and facilitating transactions by a sanctioned North Korean entity had 25 different bank accounts targeted for forfeiture.[14] Despite "no allegations of wrongdoing by the U.S. correspondent banks or foreign banks that maintain these accounts[,]" the investigation and disruption caused to those banks by the investigation is a risk that perhaps could have been avoided by stronger CDD programs.[15]

Additional 2016 enforcement actions have focused on international fraud schemes that used dozens of people, hundreds of accounts, and thousands of financial instruments.

Defendants in an Indian call center allegedly duped American citizens into paying fictitious fines to U.S.-based co-conspirators who immediately laundered the fraud proceeds by flipping them into prepaid debit cards or international wire transfers.[16] Complicating matters for the compliance efforts of the financial institutions linked to the debit cards and transfers, the "prepaid debit cards were often registered using misappropriated personal identifying information of thousands of identity theft victims, and the wire transfers were directed by the criminal associates using fake names and fraudulent identifications."[17] In October, DOJ announced that a total of 61 entities and individuals were indicted, with at least 21 individuals arrested and now awaiting extradition or trial.

Similarly, in September, DOJ charged several direct-mailing companies with fraud for soliciting phony "processing fees" from citizens duped into believing they won the lottery.[18] The Canadian payment processor for these mailers was also targeted because of its alleged knowledge of the frauds perpetrated by its customers, with the U.S. Office of Foreign Assets Control ("OFAC") taking the extraordinary step of designating the payment processor and numerous related entities and individuals as members of a significant transnational criminal organization — a designation typically reserved for terrorist networks and drug cartels.[19] Accounts associated with these sanctioned entities are being seized around the world (albeit in forfeiture proceedings that are currently being contested), and legitimate financial institutions are continuing to enhance their CDD programs to detect and report assets by the sanctioned entities themselves, as well as suspicious activities arising from potentially related parties or schemes.

Civil enforcement actions in 2016 have also focused on entities doing business across borders in high-risk industries that often involve receiving large amounts of cash, aggregating funds, or maintaining nested accounts for the banked industry's own customers. For instance, the gaming industry has been a heavy focus of FinCEN. From April 2016 to October 2016, all reported FinCEN enforcement actions have been against gaming industry participants.[20] Both U.S. federal and state enforcement agencies have targeted daily fantasy sports and other online gaming entities for investigation, issuing a number of grand jury subpoenas and civil investigative demands. The EU's Fourth AML Directive has expanded the compliance requirements for a variety of gaming industry participants. These developments have led some depository institutions and payment processors serving the gaming industry to employ heightened due diligence and to conduct independent investigations of the legality of the gaming that occurs, as well as of the identities of the gaming participants.

CONCLUSION

The added responsibility of CDD makes it more difficult for bad actors to use nested accounts, gaming transactions, prepaid cards, digital currencies, and shell corporations to launder money or finance terrorism. With these new regulations being enacted across the globe, financial institutions are expected to analyze, investigate, and report more information to law enforcement than ever before. Fairly or unfairly, financial institutions are tasked with collecting information on the beneficial owner of its customers — information the government has been unable to easily compile in the past — as well as monitoring those beneficial owners for any AML violations. Complete de-risking is likely discriminatory and certainly problematic from a global compliance perspective, but complete acceptance of business accounts serving nested customers or geographically risky areas is likely an AML failure.

Governments ultimately will find it far easier to prosecute deep-pocketed financial institutions within their own borders for ineffective CDD efforts than to chase down ultimate bad actors. With both regulatory attention and criminal and civil enforcement efforts across the globe directed toward these enhancements to AML programs, financial institutions should seek experienced counsel in updating, independently auditing/testing, and investigating high-risk scenarios flagged by their AML programs.

Notes:

[1] Financial Industry Playing the Role of Law Enforcement, Thomson Reuters (November 2016).

[2] "Correspondent banking is the provision of banking services by one bank (the 'correspondent bank') to another bank (the 'respondent bank')." FATF Guidance, *Correspondent Banking Services*, *t* http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf, October 2016.

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *See* EUR-Lex Summary of Legislation, http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:32015L0849.

[10] *Id.*

[11] Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29397 (May 11, 2016) (final rule) (to be codified at 31 C.F.R. pts. 1010, 1020, 1023, 1024, & 1026).

[12] For more information on the new FinCEN CDD Requirements, *see* FinCEN Adopts New Customer Due Diligence Requirements for Financial Institutions, http://www.klgates.com/fincen-adopts-new-customer-due-diligence-requirements-for-financial-institutions-07-26-2016/.

[13] *See* https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital.

[14] *See* https://www.justice.gov/opa/pr/four-chinese-nationals-and-china-based-company-charged-using-front-companies-evade-us.

[15] *Id.*

[16] *See* https://www.justice.gov/opa/pr/dozens-individuals-indicted-multimillion-dollar-indian-call-center-scam-targeting-us-victims.

[17] *Id.*

[18] *See* https://www.justice.gov/opa/pr/justice-department-and-law-enforcement-partners-announce-civil-and-criminal-actions-dismantle.

[19] *Id.*

[20] *See* https://www.fincen.gov/news-room/enforcement-actions.

KEY CONTACTS

MARK A. RUSH
PARTNER

PITTSBURGH, WASHINGTON DC
+1.412.355.8333
MARK.RUSH@KLGATES.COM

JUDITH RINEARSON
PARTNER

NEW YORK, LONDON
+1.212.536.3928
JUDITH.RINEARSON@KLGATES.COM

STEFANIE M. LACY
ASSOCIATE

PITTSBURGH
+1.412.355.8691
STEFANIE.LACY@KLGATES.COM

