Special Report: What FinTechs Need To Know About AML

Beginning in 1950 with the founding of the Office of Foreign Assets Control ("OFAC") and continuing to the present with the recent passage of the Anti-Money Laundering Act of 2020, the US enacted a complex set of overlapping laws, rules and regulations that require financial institutions ("FIs") to take steps designed to detect and prevent money laundering and terrorist financing (the "AML Laws"). Without detailed knowledge of the AML Laws, it's all too easy to miss a key requirement and incur significant regulatory fines, business disruption and reputational damage.

DigiPli - together with Barclays Rise - prepared a series of four articles (consolidated here into one) designed to help FinTechs operating in the US understand their AML obligations and avoid costly mistakes.

PART 1: THE WHO AND THE WHAT

Who's subject to the AML Laws?

The AML Laws apply to more than just traditional financial institutions such as banks, broker-dealers, and commodity firms. FinTechs that operate as non-bank financial institutions ("NBFIs") are also "financial institutions" as defined in the AML Laws. This includes cryptocurrency exchanges, operators of credit card systems, insurance companies, online lending and finance companies, P2P lenders and transferrers, money service businesses, FX dealers, crowd funding platforms and others.

What are the main requirements of the US AML Laws?

Every FI – including FinTechs operating as NBFIs – must establish an AML program comprised of four main 'pillars'. However, the more highly regulated FIs (e.g., banks, broker-dealers, and others) are also subject to a fifth pillar, which is discussed later.

The four main AML pillars applicable to all FIs are:

1. *Appoint an AML Officer.* Designate an individual who's responsible for overseeing AML compliance for the FI. They must have both sufficient knowledge of the AML Laws, and sufficient authority within the organization to ensure they can effectively perform their duties.

2. *Implement AML Controls.* Establish, document, and implement internal processes, policies, controls, and systems reasonably designed to comply with the AML Laws, in a manner that's tailored to the FI's business and operations ("AML Controls"). The AML Controls and associated documentation must also be periodically reviewed to ensure they remain current and effective. Details as to this pillar – the most complex, costly and time-consuming one – are discussed in Part 2 below.

3. *Provide Employee Training.* Periodically train all employees about the AML Laws, and their responsibilities in ensuring the AML Controls are effectively implemented. The training must be tailored to a particular FI's AML Controls, attendance must be documented, and 'off-cycle' training should be provided if the AML Controls materially change.

4. *Perform Independent Testing.* On a periodic basis (most FIs do this at least annually) an independent party must test the effectiveness of the AML Controls. The testing doesn't need to be performed by a third-party audit or consulting firm. However, the person(s) performing the testing must be knowledgeable and qualified regarding the AML Laws, and they cannot be responsible for AML compliance at the firm.

PART 2: REQUIRED AML CONTROLS

This "second pillar" of the AML Controls is the most complex, time-consuming, and resource-intensive aspect of an AML program. A FinTech operating as an NBFI must at a minimum implement the following controls:

1. *Customer Identification*. Verify each customer's identity through either documentary (reviewing an ID card) or non-documentary (reviewing / accessing other available information) means to confirm their: (a) name, (b) address, (c) EIN/TIN/SSN and (d) for individuals, date of birth. The FinTech must also notify the customer that they will be performing this verification by sending them a 'CIP Notice'.

2. *Sanction Screening*. Ensure that the customer is not on one of OFAC's sanction lists. The check should be performed both prior to opening the account, and periodically during the relationship to ensure that the customer is not added to an OFAC list after account opening. Similarly, when sending funds or digital assets on behalf of a customer to a third-party recipient, the FinTech must confirm that the recipient is not on one of OFAC's sanction lists.

3. *Transaction Monitoring*. Develop and implement processes and systems designed to detect activity that may be indicative of money laundering or other criminal activity. Given the readily available nature of automated systems, regulators repeatedly found reliance on manual reviews of spreadsheets to be an "unreasonable" way to conduct transaction monitoring.

4. *SAR Reporting*. Report suspicious activity that might indicate money laundering, tax evasion, or other criminal activities to the Financial Crimes Enforcement Network ("FinCEN") within 30 days of detecting the suspicious activity.

5. *CTR Reporting*. Depending on the FinTech's business, file Currency Transaction Reports for currency transactions over $10,000 in the aggregate conducted by, or on behalf of, a customer during a single day.

6. *Record Keeping & Retention*. Depending on the FinTech's business, maintain records of each currency transfer of $3,000 or more, along with certain related information such as name, address, customer account number, date and amount of transfer and name and account information of the recipient. This requirement (the "Travel Rule") also requires that some of this information "travel" with the transmittal order through the payment chain to the recipient's FI. Note that FinCEN is seeking to amend the record-keeping requirements and the Travel Rule applicable to cryptocurrency firms. However, due to intense push-back from the industry, coupled with the Biden administration suspending certain rule-making activities, FinCEN's proposed amendments have been on hold since January.

7. *FinCEN Registration*. FinTechs that are money service businesses ("MSBs") must, in addition to complying with state licensing requirements, register with FinCEN within 180 days after being licensed as an MSB. They must also renew their FinCEN registration every two years.

8. *Responding to Information Requests*. Depending on the FinTech's business, FinCEN may, pursuant to Section 314(a) of the PATRIOT Act, either on its own behalf or on behalf of federal, state, local or international law enforcement, request information from FinTechs about accounts and transactions of persons that may be involved in terrorism, money laundering or other criminal activity. FinTechs must comply with, document and retain any FinCEN information requests they receive.

PART 3: ADDED REQUIREMENTS FOR HIGHLY REGULATED FINANCIAL INSTITUTIONS

FinTechs operating as banks, mutual funds, broker-dealers in securities, futures commission merchants, and introducing brokers in commodities ("Highly Regulated FIs") are subject to all the requirements as FinTechs operating as NBFIs, as discussed above. However, they're also subject to an additional set of requirements often referred to as the 'fifth pillar.'

The CDD Rule

The additional requirements applicable to Highly Regulated FIs arise out of the Customer Due Diligence Rule (the "CDD Rule"), which applies to all customer accounts these FIs open on or after May 11, 2018. The CDD Rule requires Highly Regulated FIs to implement the following additional requirements for each customer:

1. *Beneficial Ownership Identification.* Identify and verify the identity of the 'beneficial owners' and 'control persons' of each customer that is a legal entity.

2. *Nature & Purpose Analysis*. Collect information that will enable the FI to understand the nature and purpose of the customer relationship by considering factors such as geography, product type, expected account value, expected frequency of transactions, customer type, etc. The FI must use this information to assign an AML-specific risk rating to a customer (i.e., the risk of the customer using the FinTech's infrastructure to engage

in money laundering, criminal activity, or terrorist financing activities) and perform enhanced due diligence on higher risk customers.

3. *Ongoing Customer Monitoring*. Conduct ongoing monitoring of the customer's activities to identify and report suspicious transactions and, with a frequency driven by the customer's risk rating, periodically review and update the customer's assigned risk rating, profile, and other information.

Note that some commentators believe the Fifth Pillar applies to NBFIs as well. There's language in the Federal Register adopting the CDD Rule, which characterizes these requirements "as nothing more than an explicit codification of existing expectations." This suggests that FinCEN may take the position that all FIs should have already implemented this requirement – whether or not that's explicitly stated in the law.

Additional AML Requirements

Depending on the type and nature of a Highly Regulated FI's business, operations and regulatory status, additional AML-related requirements may apply to the FinTech. Many of these requirements are covered in the next section, which addresses AML best practices for FinTechs operating as NBFIs.

PART 4: BEST PRACTICES

This final section covers AML best practices for FinTechs operating as NBFIs, which may go above and beyond what's specifically required by the AML Laws.

Why do more than the AML Laws require?

Once they begin to scale or seek external funding, many FinTechs operating as NBFIs implement AML best practices above and beyond what's specifically required by the AML Laws. This is prompted by several considerations.

1. *Risk Mitigation*. Given the risk of massive fines, coupled with the fact that a FinTech's management can be held personally (and criminally) liable for violating the AML Laws, the cost of 'getting it wrong' is huge. Plus, given that regulators will view any failure with 20-20 hindsight, taking additional steps to mitigate potential AML risk is important to both investors and management.

2. *Avoiding Reputational Damage*. If a FinTech's infrastructure is ultimately found to have been used to launder illicit funds, regardless of the legal requirements this will both cause reputational damage and increase the risk of a regulator questioning whether the FinTech's AML controls were reasonably designed. This can adversely impact company valuations, customer retention and public perception.

3. *Integration with Highly Regulated FIs*. FinTechs seeking to integrate with banks, broker-dealers or other Highly Regulated FIs may be expected (or even contractually required) to implement AML controls similar to those applicable to the more highly

regulated entities. Failure to do so may impact a FinTech's ability to scale or enter into valuable partnerships.

4. *Non-US Operations*. Many non-US AML laws, along with international standards published by the Financial Action Task Force ("FATF"), impose standards that are stricter than US AML Laws. Accordingly, some FinTechs with a global footprint choose to universally implement AML controls designed to meet the standards of FATF and all other jurisdictions in which they operate.

What industry best practices should FinTechs adopt?

What constitutes AML-related 'best practices' is constantly evolving to adapt to changes in the markets, technology and the political environment. While not an exhaustive list, many FinTechs operating as NBFIs implement some or all of the below best practices – regardless of whether they're technically required by the AML Laws:

1. *The CDD Rule*. Many FinTechs implement the CDD Rule, i.e., the 'fifth pillar' applicable to Highly Regulated FIs discussed in the prior section. When implementing the CDD Rule, FinTechs place particular emphasis on: (a) risk-ranking customers using AML-relevant criteria, (b) performing enhanced due diligence ("EDD") on higher risk customers and (c) periodically reviewing and updating customers' risk ratings, profiles, and other information.

2. *Non-US Sanction Lists*. Screening customers (and recipients to whom customers are sending funds or digital assets) to determine whether they are on non-US sanction or watch lists. The most used global lists against which customers are screened are the UK, UN, and EU sanctions lists.

3. *Politically Exposed Persons*. Screening customers to determine if they are Politically Exposed Persons ("PEPs") who are foreign governmental officials and their family members and associates. PEPs are generally considered higher risk customers from an AML perspective. Many FinTechs perform EDD on PEPs.

4. *Negative News*. Running searches on customers to determine whether they were publicly reported as being engaged in criminal, fraudulent or other similar activities, which, depending on the activity, may impact the customer's risk rating.

5. *Other High-Risk Screening*. Running searches on customers to determine whether they are: (a) on government enforcement or watch lists, (b) a State Owned Enterprise (generally deemed higher risk) or (c) a higher risk type of business (e.g., a marijuana-related business). Again, inclusion on one of these lists may impact the customer's risk rating.

6. *AML Risk Assessments*. Performing a periodic (most FIs do this annually) AML risk assessment to assist the FI in identifying emerging AML-related risks due to a change in: (a) applicable laws or rules, (b) the political or regulatory environment, or (c) the

FinTech's own business activities. The results of the Risk Assessment are then used to update the AML controls.

Again, while not explicitly required by law, FinTechs that implement some or all of these best practices will have a much stronger legal and regulatory position if it's later found that a criminal used their infrastructure to facilitate illicit transactions.

Further Insights

While this article focused on the AML Laws, many other regulatory requirements apply to FinTechs. These include federal and state registration and licensing requirements, customer complaint requirements, whistle-blower policies, anti-bribery policies, requirements under the Unfair, Deceptive or Abusive Acts or Practices (UDAAP) rules, and others. Proactively addressing the AML Laws, in addition to other regulatory requirements, early in a FinTech's lifecycle will reduce risk in the long term, and help the FinTech establish the proper foundation to scale and integrate with other regulated financial institutions more quickly and efficiently.

Conclusion

Designing and implementing an AML program that meets regulatory requirements in an efficient and effective manner is a complex and daunting task for many FinTechs. If you have any questions regarding your AML obligations, or if you're looking to automate your AML program and streamline your customer experience, contact us at team@digipli.com.