



## 2018: AML compliance retains high importance in FINRA and SEC exam priorities

With the fall examination cycle in full swing, we thought it would be prudent to revisit the 2018 examination priorities set forth by the US Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) in their respective examination priorities letters.<sup>1,2</sup> Both the SEC and FINRA explicitly identified specific examination

priorities for Covered Financial Institutions<sup>3</sup> (hereafter firms). In addition, FINRA published the Report on Examination Findings, 2017<sup>4</sup> (Examination Findings Report) and noted in its examination priorities letter that the report includes observations on concerns and effective practices relevant to areas identified in the 2018 priorities letter. Across the priorities letters and the

FINRA Examination Findings Report, the regulators detail four priorities: the Customer Due Diligence (CDD) program; a tailored risk assessment; transaction monitoring surveillance controls and timely, accurate reporting of identified suspicious activity; and independent testing of the firms' anti-money laundering (AML) programs.

<sup>1</sup> FINRA 2018 Regulatory and Examination Priorities <http://www.finra.org/industry/2018-regulatory-and-examination-priorities-letter>

<sup>2</sup> SEC 2018 National Exam Program Examination Priorities <https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf>

<sup>3</sup> 31 CFR 1010.100(t)

<sup>4</sup> Report on FINRA Examination Findings, 2017 <http://www.finra.org/industry/2017-report-exam-findings>

### Customer identification/due diligence and FinCEN's CDD rule

The first priority highlighted by the SEC and FINRA (collectively, the regulators) is the new CDD rule. The driving force behind the first priority was the Financial Crimes Enforcement Network's (FinCEN) finalization of the long awaited CDD rule on May 11, 2018, which is now considered the "fifth pillar."<sup>5</sup> Accordingly, the regulators were consistent on the components of CDD, with FINRA going one step further and explicitly noting them: (1) customer identification and verification; (2) beneficial ownership identification and verification; (3) understanding the nature and purpose of customer relationships; and (4) ongoing monitoring for reporting suspicious transactions, and, on a risk basis, maintaining and updating customer information.

Given that the SEC listed CDD as its first AML priority, and the extent to which FINRA quoted the FinCEN CDD rule, one can infer the regulators prioritized CDD for firms. While existing Customer Identification Program requirements, representing the first CDD component, have remained unchanged from 2001,<sup>6</sup> the new CDD rule reiterates the obligation. In addition, the remaining components of the CDD rule can be summarized as a firm's ability to illustrate how it knows its customers through beneficial ownership analysis, determination of economic purpose, and identification of deviations from expected behavior, respectively. The regulators suggest accomplishing this customer understanding by developing customer risk profiles and implementing specific transaction

monitoring surveillance controls based on those customer risks.

### Tailored risk assessment

The regulators' second identified priority is examining how firms create a tailored risk assessment that is specific to the firms' business profiles (e.g., customers, products, and geographies.) FINRA referenced its Examination Findings Report for firms to understand how to assess risk and effective control practices related to tailoring a risk assessment. This report identified deficiencies where, for example, a firm's business growth and new risks were not addressed in its AML program. This was particularly apparent where firms' businesses had grown to offer additional high-risk products or evolved and firms did not update their AML risk assessments to sufficiently identify and control for new risks. The regulators expect that firms commence quantifying the risks of new products and services upon offering them to their customers. The regulators' letters both include the emerging risks presented by cryptocurrencies and initial coin offerings (ICOs) to illustrate the expectation that firms quantify the new risk in their business model and implement associated controls. The FINRA Examination Findings Report noted that firms with effective AML programs incorporate the quantification of risks and mitigating controls into their AML programs, one that is tailored to the firm's business model as opposed to simply implementing a more "generic" program.

Further, as firms document and assess their tailored risks, the regulators then expect the firms to

demonstrate controls, in particular with specific transaction monitoring surveillance for the identified risks. FINRA assesses the adequacy of firms' transaction surveillance programs to ensure that they have transaction monitoring system rules in place to enable monitoring of any new high-risk products and services such as cryptocurrencies and ICOs.

### Transaction monitoring and suspicious activity reporting

The regulators' third priority is to conduct ongoing monitoring based on the firms' identified risks and to file timely and accurate suspicious activity reports (SARs). FINRA noted that it continues to find deficiencies related to the adequacy of firms' resources as well as their policies, procedures, and practices for detecting and reporting suspicious transactions. Firms are required to file SARs with FinCEN when potentially suspicious activity is detected and the SEC examination priorities letter indicated a focus on whether firms are filing timely, complete, and accurate SARs with FinCEN once firms detect any suspicious activity.

Firms need to adapt transaction monitoring rules designed to identify potential sales of unregistered securities to include cryptocurrencies and ICO transactions when they are considered securities, as both regulators highlighted review of compliance with securities laws with respect to those products. FINRA noted that firms need to incorporate transaction monitoring for foreign affiliates that conduct high risk transactions, such as microcap securities and dual currency transactions. Finally, FINRA advised

<sup>5</sup> Customer Due Diligence Requirements for Financial Institutions <https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer->

[due-diligence-requirements-for-financial-institutions](#)

<sup>6</sup> See 31 CFR 1024.220 (Customer identification programs for broker-dealers) and 31 CFR 1026.220 (Customer identification programs for mutual funds)

firms to confirm that transaction monitoring includes securities-back lines of credit, including aggregation across multiple accounts.

### Bank Secrecy Act (BSA)/AML independent testing

The regulators identify independent testing as the final priority. Firms must perform independent testing of the entire AML program, including the risk and controls for the above priorities. The SEC assesses firms' independent testing to confirm it is "robust and timely." FINRA pointed to its Examination Findings Report and two specific failures with independent testing: it did not adequately assess implementation of the firm's AML program and/or where it occurred less frequently than warranted based on the firm's business model. The regulators also state that BSA/AML independent testing should evaluate the CDD program including the firm's risk-based approach to collecting and updating customer information. The testing should also examine whether the suspicious activity detection and reporting program is based on

firm-specific risks and is updated for newly offered products and services, including cryptocurrency and ICOs.



### Conclusion

Both the SEC and FINRA are aligned in their exam priorities, focusing on four AML program core principles— understanding of the customers; identifying risks within firm business profiles; controlling for the risks through transaction surveillance; and conducting independent testing of the AML program.

Firms should understand its current business model including changes to products offered (e.g., cryptocurrencies and ICOs) and adapt their AML program accordingly. In addition, firms should not lose sight of prior examination results including independent testing to assess and ensure programmatic effectiveness. Where business changes necessitate or when examinations identify deficiencies, firms must promptly apply corrective action and incorporate necessary changes to policies, procedures, and controls.

**For further information, visit our website at [www.deloitte.com](http://www.deloitte.com)**

### Contacts—For more information, please contact:

#### Joshua Hanna

Principal | Deloitte Risk and Financial Advisory  
Deloitte Transactions and Business Analytics LLP  
+1 404 220 1336  
[jhanna@deloitte.com](mailto:jhanna@deloitte.com)

#### Brian Peres

Senior Manager | Deloitte Risk and Financial Advisory  
Deloitte Transactions and Business Analytics LLP  
+1 571 882 6526  
[bperes@deloitte.com](mailto:bperes@deloitte.com)

#### Jennifer Flannery

Manager | Deloitte Risk and Financial Advisory  
Deloitte Transactions and Business Analytics LLP  
+1 212 436 3786  
[jflannery@deloitte.com](mailto:jflannery@deloitte.com)

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

#### About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.

Copyright © 2018 Deloitte Development LLC. All rights reserved.