



Anti-money laundering in the post-CDD era

How the new Customer Due Diligence
rule impacts anti-money laundering in the
years to come



genpact

Transformation
Happens Here

Tens of thousands of hours of preparation have gone into the policies, procedures, and technologies needed to effectively respond to the Financial Crimes Enforcement Network's (FinCEN) Customer Due Diligence (CDD) rule. Since the rule was announced in May 2016, every anti-money laundering (AML) industry conference, peer working group, and compliance department planning meeting has focused extensively on CDD rule preparations. Now that the rule is in effect as of May 2018, what comes next will require AML programs to have a solid plan to operationalize this data to improve overall compliance.

The CDD rule examined

The CDD rule lays out, for the first time, the four core elements of customer due diligence that FinCEN says should be requirements of all AML programs at institutions covered by the rule, which include federally regulated banks and federally insured credit unions, mutual funds, brokers or dealers in securities, futures commission merchants, and introducing brokers in commodities.

These elements are:

- 1. Customer identification and verification**, which has long been a standard part of “know your customer” programs but will likely involve increased collection of identification documents and growing reliance on third-party data providers for verification services.
- 2. Beneficial ownership identification and verification**, which is an expansion over previous requirements. This somewhat controversial element significantly expands data collection and research needs of financial institutions with regard to legal entity customers.
- 3. An understanding of the nature and purpose of customer relationships to develop a customer risk profile.** This necessitates the development of a risk matrix for use in evaluating customer risk that incorporates reliable customer data, along with other financial activity information.
- 4. Monitoring and reporting suspicious activity and also updating customer information on a risk basis.** This longstanding requirement ties together the other three elements by requiring that the first and second are updated based on the results of the third.

Of the four elements, FinCEN notes that the first is already an explicit AML program requirement, while the second is new and the last two are both implicit requirements now being made explicit. As a whole, the rule has two major requirements: collecting reliable information on customers and using that customer information to evaluate risk and improve AML processes.

In order to maintain regulatory compliance and reduce negative customer impacts, firms should consider ways in which they can automate manual due diligence processes and implement a CDD approach that allows for increased agility and responsiveness to change.

-ACAMStoday.org

(Magazine for AML professionals)

What to do with all the data?

Going beyond compliance by understanding how to use new data to enable automation for your AML program

So much time has been spent focusing on the “new” part of the CDD rule - the beneficial ownership requirement to collect previously uncollected information - that many financial institutions’ AML programs view the rule as a “new data collection requirement.” While this is certainly true, collecting information is only half of the rule - and, arguably, not the important half. In the eyes of FinCEN and other agencies, the more pivotal part of the rule is how that information is ultimately used.

To FinCEN, having the correct information is not the goal of AML, although proper record-keeping does support law enforcement investigations. Instead, the goal of AML is to properly detect risky customers conducting suspicious activity. The information collection is only a means to an end - better information collection means better customer risk profiles, which means better transaction monitoring and better suspicious activity reporting. The end result is better leads for law enforcement and regulators.

While all covered financial institutions likely have sophisticated (or at least, hopefully, passable) plans to comply with the data collection portion of the CDD rule as of May 2018, certainly fewer have a solid plan for operationalizing this data to improve AML compliance. Given its explicit inclusion in the rule, the most prominent use is likely through some form of customer risk profiling. But risk profiling exists on a spectrum. On one end of this spectrum is a simple methodology that manually compiles a risk profile using a small number of defined risk indicators, like account type, Politically Exposed Person status, and previous Suspicious Activity Report filings. On the other end of the spectrum is an automated customer risk scoring algorithm that accounts for dozens of risk indicators and dynamic updates with changes to customer information or behavior. As new data is collected, the latter will increasingly become the expectation of regulators—given the focus of the rule on updating customer risk profiles based on changing behavior.

Manual vs. Automated

A manual option may allow a financial institution to establish basic compliance, but truly operationalizing the full force of the CDD rule is unlikely without the proper technology designed to enhance automation. Automation technology allows data to be ingested more quickly. If more cutting edge options, such as Big Data technologies, are also applied, this data ingestion can be done even more quickly and efficiently as there would not be a requirement to structure the data before it's ingested.

More importantly, automation also allows for the ability to conduct value-added analysis. For example, the data set could be enriched with risk ratings based on customer profiles that could be used to stratify and tune transaction monitoring sensitivities. Taken a step further, by using advanced analytics and/or machine learning, transaction monitoring alerts could then be prioritized to focus limited human analytical resources on the most risky alerts first. The result? Economy of effort and operational effectiveness.

"Making anonymous companies a relic of the past will help create a global financial system that's transparent and accountable and that works for everyone."

- The financial transparency coalition



New data, new expectations

Understanding the new expectations for your AML programs in the coming years

Beyond operationalizing data, what other post-CDD expectations will be placed on covered financial institutions?

Post-CDD, law enforcement will most likely increase requests for beneficial ownership information of legal entities. FinCEN and other agencies are essentially using the CDD rule as a back-door way to improve transparency of business ownership without having to battle legislatively with states like Delaware and Nevada that benefit from corporate opacity.

While other data sources will likely catch up in time after the CDD rule goes into effect, covered financial institutions will likely be the best source of beneficial ownership information for law enforcement in the interim. This will mean more subpoenas and other requests simply to gather legal entity information. In the long term, manual solutions will impede the ability to quickly and accurately consolidate data to respond to these requests and maintain compliance.

Increased beneficial ownership information will also impact the AML responsibility of sanctions screening. New ownership information will not only mean additional parties to screen, but also the possibility of previously unknown ownership stakes by sanctioned parties. While minority ownership stakes by sanctioned entities do not necessarily make a business sanctioned, the Office of Foreign Assets Control's (OFAC) 50 percent rule does state that a legal entity that is owned 50 percent or more by one or more sanctioned entities is itself sanctioned, even if the legal entity is not explicitly on the Specially Designated Nationals and Blocked Persons list. Further, OFAC has recommended that financial institutions consider the potential sanctions risk of entities that are controlled by Specially Designated Nationals that only hold a minority stake - adding yet another level of nuance to the responsibilities of sanctions screening programs. So far, enforcement of the 50 percent rule has been very limited, but increased awareness of beneficial ownership stakes will likely expose additional avenues for sanctions enforcement violations. The enhanced clarity around beneficial ownership will require AML programs to potentially revisit their policies and risk assessments, as well as potentially tune their screening rules.

Finally, clarity on beneficial ownership may increase the focus on tax evasion, and bring about more successful prosecution, by more clearly linking owners to assets and therefore tax responsibilities etc. The CDD rule provides a critical data point, owner identity, to enable US efforts to increase financial transparency and combat financial crimes such as money laundering and tax evasion. The CDD rule will provide additional force to many international

agreements with a greater ability to identify absconders early on, presumably reducing the time, cost, and resources required. In this regard, the CDD rule's timing is impeccable, considering the UK recently announced it would also require enhanced beneficial ownership reporting in its overseas territories, such as the Cayman Islands and British Virgin Islands. The ability to have a robust, single view of the customer - one that enriches transaction monitoring and screening systems with customer profile data, transaction, and external data such as negative news - will become more important.

Conclusion

The US is entering a new phase of AML compliance now that the CDD rule has gone into effect as of May 2018, with new expectations from regulators and law enforcement. Two years have been spent preparing to comply with the rule and its specific elements; however, far less time has been spent identifying what comes next now that FinCEN has defined these four core elements of AML compliance. With a vast amount of new data coming in and the complexity of the requirements, technology will be key for both managing data and responding to it effectively and efficiently.

About Genpact

Genpact (NYSE: G) is a global professional services firm that makes business transformation real. We drive digital-led innovation and digitally-enabled intelligent operations for our clients, guided by our experience running thousands of processes primarily for Global Fortune 500 companies. From New York to New Delhi and more than 25 countries in between, we connect every dot, reimagine every process, and reinvent companies' ways of working. [Transformation happens here.](#)

For additional information visit <https://www.genpact.com/risk-compliance/risk>

Get to know us at [Genpact.com](#) and on [LinkedIn](#), [Twitter](#), [YouTube](#), and [Facebook](#).

© 2019 Genpact, Inc. All rights reserved.

