Statement of

John J. Byrne, Esq., CAMS

President

Condor Consulting, LLC

Before

The House Subcommittee on Terrorism and Illicit Finance

And the

House Subcommittee on Financial Institutions and Consumer Credit

November 29, 2017

To the Chairmen and members of the subcommittees, I am John Byrne, President of Condor Consulting LLC and the previous Executive Vice President of ACAMS (Association of Certified Anti-Money Specialists). I am extremely fortunate to have been part of the AML (anti-money laundering) community for over thirty years. Whether it has been with the financial sector, or representing the entire community with ACAMS [i], it is clear to me that the private and public professionals who comprise compliance, risk, legal, advisory or regulatory oversight in financial crime prevention functions are all dedicated to stopping the flow of illicit funds. We may disagree with how to achieve this collective goal, but no one can challenge the commitment of all of those involved. It is therefore so important that as improvements are considered to what constitutes the AML infrastructure, all participants are actively consulted. The subcommittees deserve credit for reaching out on your proposal to modernize a series of requirements that are in need for revision and enhancement.

As we all are aware, the statement of purpose to the Bank Secrecy Act (BSA) in 1970 and as amended in 2001 is:

"to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism."

The key is a "high degree of usefulness" a concept that needs this serious review. I have seen, all too often, that the focus under these laws appears to be mainly regulatory compliance and NOT getting immediate access to law enforcement information for investigations and deterrence of criminal abuse of our financial system. As I cover the provisions of the proposal on "Counter Terrorism and Illicit Finance Act" and the "End Banking for Human Traffickers Act of 2017," it is important to note the following:

- Any changes in reporting or recordkeeping will impact current resources, systems and operations
- Information sharing, not only among financial institutions but active sharing between the government and financial institutions is the most essential method of succeeding in attacking all aspects of money laundering and financial crime
- With the vast array of crimes that depend on utilizing the financial sector, any modifications or eliminations of requirements MUST involve active and ongoing consultation with the private sector and their public sector counterparts
- Regulatory uncertainly can result in confusion on priorities, risk aversion that harms legitimate commerce, and loss of critical data to law enforcement, and
- The banking industry has already been a private sector leader in human trafficking detection and prevention, so any proposed regulatory changes need to recognize that clear fact

Modernization of CTRs and SARs (Section 2) and a formal review of both reporting requirements (Section 3)

There can be no question of the importance of data and other information for an effective AML program and environment. As we know, the financial sector is obligated, among many other things, to report cash transactions (CTRs) over $10,000 and file suspicious activity reports (SARS) on certain activities that a financial institution knows or suspects may be a violation of law or has no lawful purpose. CTRs have been part of the AML fabric since 1972, and SARS from 1996 (and prior to SARS, Criminal Referrals since 1984). There is certainly value for law enforcement in both reporting regimes, but I feel that SARS are, without a doubt, more essential to successful investigations, prosecutions and overall detection of financial crime. The subcommittees should be commended for attempting to review and improve these requirements. I would respectfully recommend, however, that there are elements in both reporting regimes beyond the dollar thresholds that should also be considered for improvement.

For example, the financial sector did aggressively advocate for raising the threshold for cash reporting due to the stagnant nature (over thirty years) of the over $10,000 reporting amount. For the various reasons that these subcommittee have identified, such as inflation and the many CTRs that clearly have no law enforcement value, the filing community sought a careful consideration of adjusting the thresholds. At the time, the law enforcement community reacted vehemently against such a move, claiming major loss of investigative data. I believed then, as I do now, that evidence does not support a broad position of all CTRs being valuable. During the previous debate, it was too difficult for the financial sector to continue the advocacy of change and now since there are so many system options for reporting cash activity, the question of how useful it will be to raise the dollar threshold is a valid consideration.

In discussing the idea of raising the reporting threshold for CTRs with a number of my industry colleagues, the recurring theme for a good number of institutions is that raising the threshold will

have little impact on burden because automated systems have been implemented to assist with the identification of reportable cash transactions and the filing of CTRs. I do not have enough data from all impacted filers to assess the pros and cons of raising the CTR filing thresholds in 2017, so if the subcommittees intend to pursue such a plan, I would encourage that all participants in the filing process, especially law enforcement stakeholders, be included in discussions around any potential change.

As for what causes the most difficulty for CTR filers in 2017, I would submit it is the "exemption" process that section 3 contemplates reviewing.

Returning to my thesis that regulatory uncertainty and changing expectations impact the financial sector more than any other portion of AML, exemptions from CTR reporting were first crafted as a sincere effort to eliminate reports that did not have a "high degree of usefulness" in detection of financial crime. Despite a concerted effort to improve the reporting infrastructure, as with other regulatory requirements, there are many examples of financial institutions being fined for administrative failings such as late registration, renewal of exemptions or lack of clarity as to what constitutes an exempted entity. As a result, it is considerably easier to simply file a CTR and avoid regulatory criticism. As numerous enforcement actions against financial institutions will attest to over the years, in many instances, institutions were not penalized for failure to file CTRs, but rather they were penalized for failure to file CTRs resulting from defective implementation of exemptions, leading to the failure to file CTRs.

To both simplify and ensure law enforcement utility, there has been a new call for dramatically changing cash reporting:

Eliminate All CTRS and have impacted financial institutions report cash activity directly to the Financial Crimes Enforcement Network (FinCEN).

With this change, law enforcement would get direct access to cash activity at the level decided by Congress, or by law enforcement with authority provided by Congress, and could develop metrics on what activities, types and other factors are important to the detection of all aspects of financial crime. Such a change quite possibly might eliminate one of the leading industry complaints that has persisted for many years – specific feedback from the government on the usefulness of the millions of CTRS filed annually. It is clear that a change this massive could not be commenced overnight, so creating several "pilot" programs may be the best option.

The subcommittees are also looking at suspicious activity reports (SARs) and propose an adjustment to the reporting thresholds there as well. Section 3 supplements the threshold increase with a direction to review many aspects of SAR reporting and utility. As with CTRs, I have a few comments on what parts of the SAR regime have caused much consternation to the filers.

I completely support the part of section 3 that looks at the continued filing of SARs. As with other issues that have occurred since the creation of SARs, ongoing activity reviews and reporting began with financial institutions innocently questioning the regulatory agencies and FinCEN as to their thoughts on filing SARS on activity that has already been reported. These innocent questions turned into regulation by fiat, based on current guidance and expectations

from regulators and FinCEN. Specifically, the financial sector sought guidance from FinCEN on the question of what to do if a SAR has been filed and there has been no follow-up from law enforcement. Here is the response from October 2000 from the SAR Activity Review:

"Repeated SAR Filings on the Same Activity

One of the purposes of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This is accomplished by the filing of a SAR that identifies the activity of concern. Should this activity continue over a period of time, it is useful for such information to be made known to law enforcement (and the bank supervisors). **As a general rule of thumb**, organizations should report continuing suspicious activity with a report being filed at least every 90 days. This will serve the purposes of notifying law enforcement of the continuing nature of the activity, as well as provide a reminder to the organization that it must continue to review the suspicious activity to determine if other actions may be appropriate, such as terminating its relationship with the customer or employee that is the subject of the filing." (underline emphasis added)

This response was never created as an obligation but rather as guidance to institutions trying to be proactive in reporting possible illegal activity. What happened? This "rule of thumb" became the so-called "90-day rule" and many filers have been formally criticized for not filing a SAR on continuing activity on Day 90.

Another equally frustrating "rule" that really takes the focus away from why SARS are valuable is how to handle the decision NOT to file a SAR. Here is language from the interagency FFIEC AML/BSA Examination Manual:

"The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the bank has an effective SAR decision-making process, not individual SAR decisions. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the bank has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, the bank should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith."

This coverage is a fair and a rationale view of the difficulty in determining when or if to file a SAR. However, later in the manual, you find this as a directive to examiners:

"SAR Decision Making

Determine whether the bank's policies, procedures, and processes include procedures for:

- Documenting decisions not to file a SAR.
- Escalating issues identified as the result of repeat SAR filings on accounts.
- Considering closing accounts as a result of continuous suspicious activity."

The first bullet has now turned into a "requirement" to have a "no-SAR SAR." Many financial institutions have openly complained about this created obligation and, once again, goes far beyond what the SAR regime is designed to cover.

As for the increase in SAR reporting thresholds, I will leave to current members of financial institutions to comment but will say that many banks file SARs in the hopes that law enforcement will start an investigation. If the dollar amounts are raised, will there be less consideration to lower dollar frauds and financial crime? Also, as we know from our law enforcement partners, terrorist financing models have often occurred at extremely low dollar amounts so will we be losing valuable financial intelligence?

The remaining directives in the bill to the Secretary of the Treasury is an eventual report on SAR related actions and do appear valuable, but I would remind the subcommittees that one topic--the placing of SARs and CTRs on the same form was already tried in the early 1990's and found to not be helpful in data gathering or reporting and did not create any less of a burden on filers. On one more point, I would strongly encourage the subcommittees that it is important that the language of who should be the participants in the reports (Treasury, law enforcement and the affected private sector) have equal input to these studies, along with the regulatory community.

Information Sharing – The Key to Effective Money Laundering Deterrence (Section 4)

The subcommittees are also to be commended for the inclusion of section 4 that fixes a long-held barrier to enhancing information sharing. The provision expands 314 (b) of the USA Patriot Act to ensure that financial institutions can now share information on actions that could be indicative of the many financial crimes (specified unlawful activities) in the money laundering statutes. The previous reading of 314 (b) was unnecessarily limiting and contrary to the original intent behind the legislation. As one who was intimately involved in numerous discussions around information sharing at the time the provision was being drafted into the USA Patriot Act, I was extremely disappointed with the final regulation that, in my opinion, severely limited institutions' abilities to share relevant and meaningful information. This is a welcome expansion and will result in more effective reporting and eventual detection of many forms of financial crime.

The additional portion of this section that requires regulations on expanded information sharing within the same multi-national institution will finally eliminate the barriers to effective risk response of activities throughout an enterprise.

Creation of a process for opinions, priorities and to encourage innovation (Sections 5-7)

With the plethora of questions on application of the various AML laws and regulations, it would be extremely useful for a process to be developed for impacted entities to seek formal opinions on how to traverse guidance, rules and laws. The banking industry has a long history of seeking clarity and I can recall asking that a "BSA Staff Commentary" be developed as far back as 2003 and most likely even earlier. A "no action" process with active consultation of the banking agencies could go a long way to prevent the "policy as rule" issues that I raised earlier in this testimony.

Section 6 on the creation of a priorities list would also be a welcome change to how the financial sector attempts to deal with all of the many financial crimes that can be reported on a SAR. I would again urge that law enforcement and of course, the impacted private sector, be active partners of any consultation on priorities.

Section 7 highlights the subcommittees recognition of the needed focus on the importance of technology to AML detection and prevention. Whether a multi-national company or a community bank, it is important that financial institutions be permitted to utilize technology to become more efficient. One of the common complaints I have heard is that all too often regulators make it difficult for financial institutions to experiment with new tools for fear of regulatory criticism during transitionary periods. This coupled with regulatory criticism for perceived failures because the "new technology" is not operating in the same way as the current, or old, technology, stymies innovation by the financial sector. This section should alleviate those problems.

Assessing Reporting Usefulness (Section 8)

Since the very beginning of the AML regime in 1986, all partners have struggled with how to prove usefulness in order to focus the laws and regulations on the shared ultimate goal---getting critical information into the hands of law enforcement and effectively managing actual risks within financial institutions. This section combines the need for measurements of effectiveness with improving feedback to the financial sector, a mission that will enhance and focus reporting. Currently, FinCEN does an admirable job of feedback with the previously mentioned SAR Activity Reviews and other SAR statistics. The hope is that the section 8 reports will provide data that will continue the collective goal of attacking financial crime in its many facets.

Beneficial Ownership and the CDD Rule (Section 9)

One of the major recent challenges to the financial sector in the AML area has been the impending CDD rule that is required to be implemented by May 2018. With the focus from the Financial Action Task Force (FATF) and the media outcry from the Panama and Paradise Papers, we know that there is universal focus on the mechanisms used to obscure beneficial ownership of corporate vehicles. The CDD rule is in response to the issue of transparency and FATF's critique of US law from the mutual evaluation process, but many have argued with the ease of corporate formation that the rule will not be enough. In addition, because even with the new rule, validation that the identified individuals are actually the beneficial owners is not required, and cannot be performed because of the lack of critical data necessary to perform such a validation, questions have been asked as to the usefulness of these new requirements. Section 9 responds both to the incomplete nature of the Rule and the need for increased transparency by requiring FinCEN to collect this information rather than financial institutions. According to the proposal, the CDD rule would be delayed until Financial Institutions could utilize the information for the purposes of complying with their CDD requirements. For background of concerns regarding the current rule, see the report from a June 2017 meeting of financial institutions hosted by ACAMS. file:///C:/Users/Owner/Desktop/The-Way-Forward-White-Paper%208-17-17.pdf A direct obligation to file with FinCEN is a welcomed proposal.

AML Impact on Financial Access

I would be remiss if I did not also reference the collateral damage that can and does occur with confusion regarding risk in today's AML regime. When the financial sector receives limited advice and counsel regarding how best to manage risk, the logical response by some financial institutions is to exit or not onboard certain classes of customers. The concept, euphemistically known as "de-risking", impacts access to the traditional banking sector and has harmed victims in conflict zones from receiving funding for water, utilities and other resources. Make no mistake that banks and other financial institutions should be free to decide if they can ultimately manage risk, but they shouldn't be forced to exit account relationships because of confusing and conflicting oversight and, unfortunately, the opinions of some examiners examining specific financial institutions that the institution should not bank a type of customer or a specific customer. These subcommittees can provide a valuable service to the AML and the broader global community by adding to the studies and reports an update to the challenges regarding financial access. I spoke on this topic in June in London, referencing the joint work between ACAMS members and the World Bank and have included my comments for consideration here. file:///C:/Users/Owner/Documents/Keynote%20Address_JohnJByrne.pdf

H.R. 2219 (End Banking for Human Trafficking Act of 2017)

Another critical part of the financial sector's proactive work in combatting financial crime is their work addressing the scourge of human trafficking. Perhaps it is partially the lack of public coverage of the financial sector, but the clear fact is that the men and women of the banking industry (and related financial institutions) have a long history of success of responding to human trafficking here in the United States and abroad. At ACAMS alone, the association has awarded recognition to financial institutions such as JPMorgan Chase and financial institutions in Canada such as BMO for working closely with law enforcement on various projects to create and enhance "red flags" and other indicators to assist in looking for and reporting possible human trafficking.[ii] Therefore, I would humbly suggest that the premise regarding financial institutions in this bill is flawed, and that the government could actually learn from their private sector partners how to improve due diligence regarding detecting this crime. If the subcommittees continue to move on HR 2219, I would respectfully ask that they be directed to work with the private sector on language and strategies regarding any new training or reporting.

Conclusion

While not specifically addressed in any of the proposed provisions, I would like to conclude by expanding on a point that I have made in my testimony today. Somewhere between the beginning days of the Bank Secrecy Act and where we sit currently, a good number of requirements from regulators have been imposed through the use of "guidance" and "regulatory expectations." The FFIEC (Federal Financial Institution Examination Council) BSA/AML Examination Manual is the most prominent example of this trend.

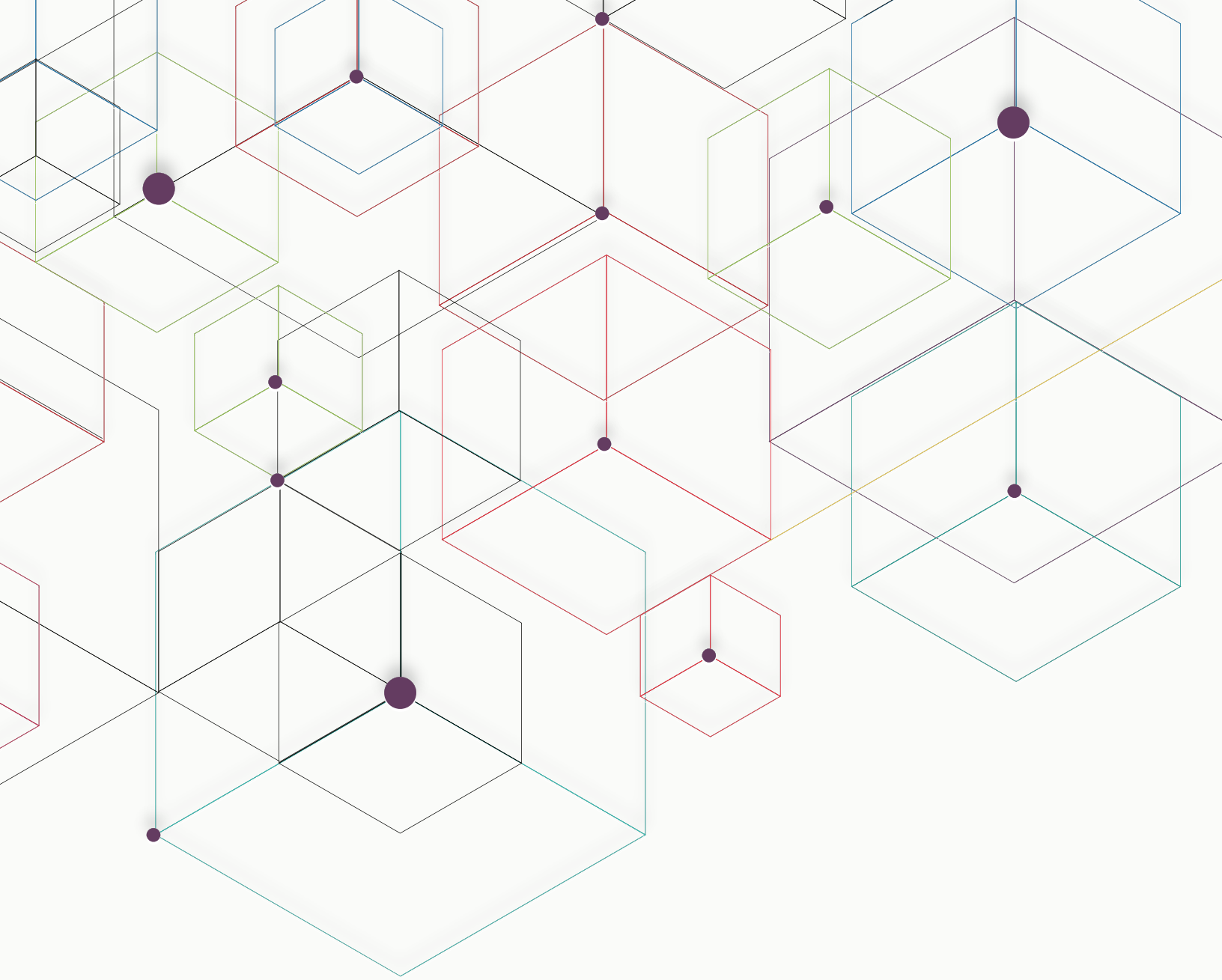
The Examination Manual, which was originally designed to provide direction to examiners while conducting BSA/AML examinations AND provide some indication to regulated financial institutions as to what should be expected during the course of such examinations has developed into requirements for regulated entities. In examination after examination, bank examiners cite the Examination Manual as the basis for requirements that banks act in a certain way. Examination reporting, including MRAs, MRIAs and MRBAs (Matters Requiring Attention, Matters Requiring Immediate Attention and Matters Requiring Board Attention) routinely cite provisions of the Examination Manual as the basis for required actions being imposed by the regulators. I would urge the subcommittees to consider whether regulatory agencies should be allowed to continue imposing "requirements" based on what was designed to provide guidance to both examiners and the industry.

I would like to thank the subcommittees for this opportunity to offer mine and my AML colleagues views on the thirty years of AML. The key going forward is to retain and support the concept of private-public partnerships. If all parts of AML work collaboratively, there is no doubt we will be successfully at pursuing and prosecuting financial criminals.

---

[i] The Association of Certified Anti-Money Laundering Specialists (ACAMS) is the largest international membership organization dedicated to enhancing the knowledge, skills and expertise of AML/CTF and financial crime detection and prevention professionals. Their members include representatives from a wide range of financial institutions, regulatory bodies, law enforcement agencies and industry sectors. http://www.acams.org/

[ii] Here is a small snippet of resources offered by ACAMS on this issue. http://www.acams.org/aml-resources/human-trafficking/



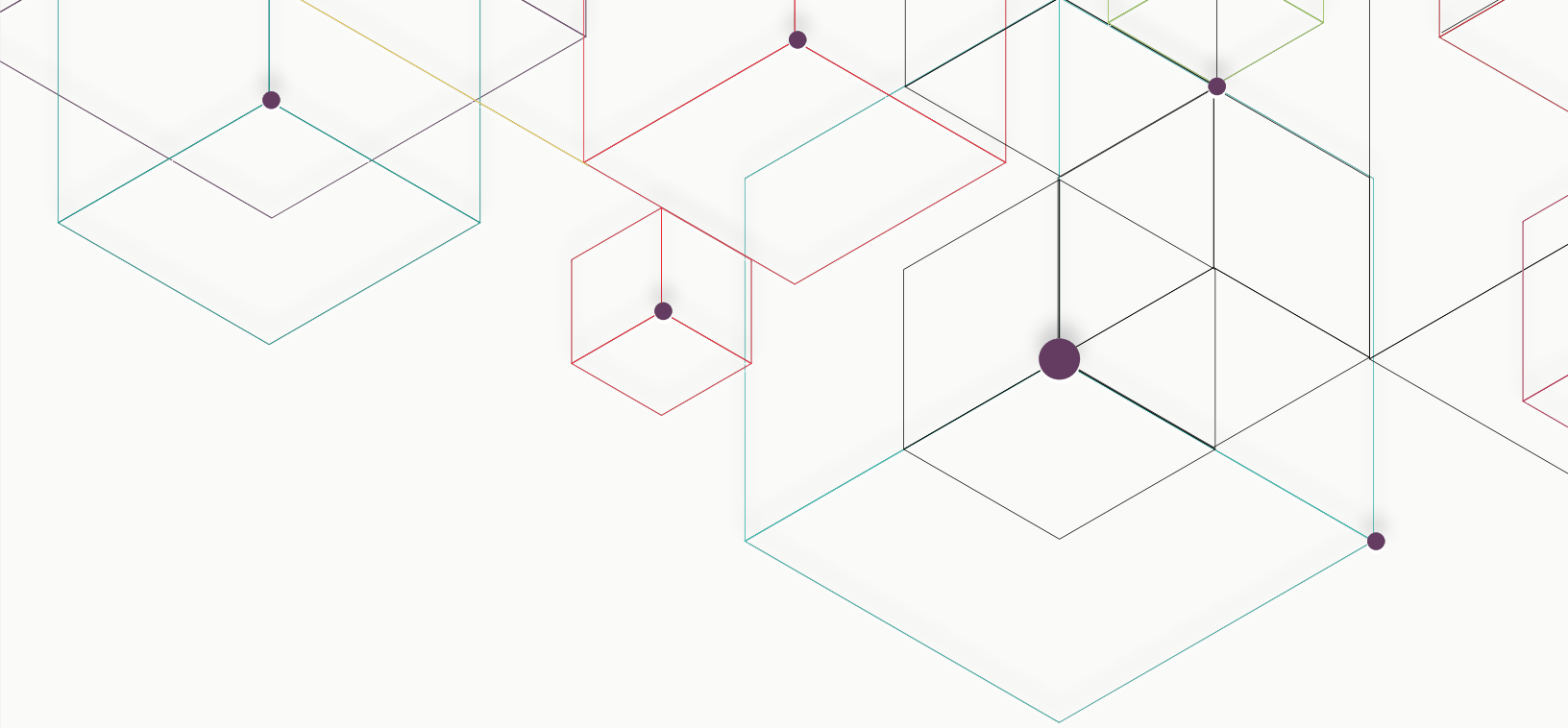
The Way Forward:

The Financial Sector Addresses the 2018 Implementation of FinCEN's CDD Final Rule

ACAMS® | Advancing Financial Crime Professionals Worldwide®

80 SW 8th St #2300, Miami, FL 33130

Telephone: (305) 373-0020; Internet: www.acams.org.



Introduction

On June 19, 2017, approximately 100 BSA/AML compliance professionals from the financial community attended ACAMS' day-long conference, "Mastering the CDD Final Rule—A Roadmap to Successful Implementation." Held in Washington, D.C., attendees represented financial institutions from across the country, ranging in size from community organizations to multi-national banks. The focus of the meeting was FinCEN's Customer Due Diligence (CDD) Requirements for Financial Institutions, published on May 11, 2016 and commonly referred to as the CDD Final Rule. The rule must be implemented by May 2018 and is intended to strengthen and clarify CDD requirements for covered financial institutions.

The bulk of the event involved roundtable-style working groups of roughly 10 members, each led by a facilitator. To foster an open dialogue, the meeting was restricted to active AML specialists who work for financial institutions; no regulators or law enforcement personnel were present. (In addition, no attendee names appear in this paper.)

This report summarizes, by subject matter, the groups' wide-ranging discussions about issues they face in implementing the CDD Final Rule. Among the topics explored were what the rule actually requires of financial institutions; navigating potential regulatory gray areas; and fashioning action plans to operationalize the rule by the May 11, 2018 deadline. Practical issues such as staffing needs, technological support and the potential impact on customer relations were also debated.

These discussions—and this paper—should not be construed as regulatory guidance or legal advice. Nor should the ideas presented be necessarily seen as a "best practices" template applicable to any or all financial institutions.

Rather, this report is intended to simply share collective insights drawn from the day's discussions. We offer them in the hope it may benefit ACAMS members as they implement this transformative rule.

The 25% Solution: Setting Beneficial Ownership Collection Thresholds

The CDD Final Rule defines two prongs for which beneficial ownership information is collected: the ownership prong and the control prong. The control prong must identify at least one individual with significant managerial control of the entity. The beneficial ownership prong requires documenting individuals who, directly or indirectly, own 25% or more equity in a legal entity customer.

Attendee discussions largely focused on operationalizing the 25% beneficial ownership requirement while maintaining a positive customer experience, and possibly adopting stricter standards depending on risk profiles.

As examples, some attendees currently collect beneficial ownership information on all 25%+ owners, regardless of risk. Others make a risk-based decision on whether to obtain that information. Other banks currently do not collect this information.

Attendees articulated a wide variety of formulas and thresholds for collecting beneficial ownership

information, currently and in the future. Some use a 15% or 10% threshold with high-risk clients. Some use a 10% threshold regardless of risk rating. One institution intends to adopt a 5% threshold for high-risk clients once the rule is implemented.

Some attendees expressed concern of a potential competitive advantage that banks with a 25% threshold might hold over banks demanding greater scrutiny. That is, a client might forgo a bank with a 10% threshold over the less intrusive 25%.

There was also discussion as to whether institutions may attract regulatory attention and/or criticism if, for instance, it applies a 25% in all cases, or creates a staggered set of thresholds below 25%. The concern is that risk criteria for adopting lower thresholds could themselves be scrutinized or second-guessed.

Other attendees felt institutions with thresholds under 25% could create a de facto standard, leading examiners to view 25% as comparatively lax. Some attendees expressed frustration that examination guidance isn't yet published. What became clear throughout this dialogue is that some FI's are already being told by examiners to go below 25%, a position contrary to all public comments on the rule from the government.

Takeaways

- While the 25% threshold is in fact already widely observed, institutions are still grappling with criteria for collecting beneficial ownership at lower thresholds
- There is concern that collecting information on owners of less than 25% could diminish the customer experience and lead clients to exit an institution
- There was broad support for examination guidance to be published sooner, rather than just before the guidance is mandatory. As most expected to roll out new systems in the first quarter of 2018, much training is needed and the timeframe is imminent

Trigger Warnings: Managing Event-Based Account Reviews

The CDD Final Rule states that ongoing monitoring shall be conducted to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including beneficial ownership. The updates would be in response to what are commonly called "trigger events." An example would be significant and unexplained changes in customer activity.

Attendees said properly responding to trigger events is a priority, but there was concern about burdensome volumes of them. Most institutions already have trigger events. The question is whether the rule could significantly increase the number of trigger events, straining management and monitoring resources.

There was some debate on how to define trigger events, as well as regulatory expectations regarding refreshment of beneficial ownership information. As examples, some institutions limit triggering primarily to new account opening. But gray areas remain. For instance, if a client adds a product or service, is that tantamount to opening a new account, and thus a trigger event, under the rule?

Others said it is important to differentiate refreshing data and updating risk profiles. A reasonable that belief ownership has changed might trigger a beneficial ownership review. A change in transactional activity, however, might be incorporated into an existing risk rating, though perhaps not require refreshing beneficial ownership.

Another issue concerned standardizing responses to trigger events. An example would be a suspicious activity report (SAR), which may or may not trigger a beneficial ownership review, depending on why it was filed.

There were multiple perspectives on managing periodic reviews, particularly on how frequently to conduct them. With many institutions, review frequency is tied to factors such as risk profile. One attendee's institution requires a regular know your customer (KYC) refresh for high-risk clients regardless of whether a trigger event occurs.

Takeaways

- Trigger events resulting from ongoing monitoring can help ensure beneficial ownership information is current, but institutions are concerned about an overabundance of them
- Attendees felt not all trigger events require refreshing beneficial ownership information but, rather, may be cause to investigate whether a risk profile should be updated
- Institutions should develop written policies and procedures for event-triggered updating, train bank personnel on them, and ensure staffing is sufficient to meet the demand

Getting On Board: The CDD Final Rule's Impact on Account Opening Practices

The CDD Final Rule is not retroactive. It applies to accounts opened after the May 2018 deadline. Covered financial institutions will be required to obtain, verify and record beneficial owners of legal entity customers.

However, some attendees are grappling with new-account regulatory framework.

One issue is the explicit requirement to maintain risk-based procedures to understand the nature and purpose of an account. Standardizing systems for determining this could be difficult, given the innumerable purposes for accounts. Some institutions plan to offer a drop-down menu of account description options, such as payroll, operations, etc. Others may ask clients for their North American Industry Classification System (NAICS) code, used by federal statistical agencies to classify business establishments.

Some said defining a new account may prove problematic. For instance, should a second account opened by an existing client be treated as new—and therefore require beneficial ownership collection? If a client adds a product or service, does this constitute a new account? Another issue is whether relying on previously collected information is acceptable. Some felt it was acceptable to rely on existing information if the beneficial owner or controlling person had an existing account. Others disagreed.

There was a similar divergence of views about account opening processes. Many attendees would not open accounts without determining beneficial ownership. Others, however, said they would consider a risk-based decision to permit opening an account, premised on there being a firm deadline—typically 30 to 60 days—for determining beneficial ownership.

> (NOTE: Guidance received from the Department of the Treasury, Financial Crimes Enforcement Network, dated 5/11/16 in the Federal Register, states: *'Because the risk-based verification procedures must contain the same elements as required by the applicable CIP rule to verify the identity of individual customers, verification must be completed within a reasonable time after the account is opened.'* Therefore, if under the written CIP rules at several financial institutions, a 30-day window (or other) may incorporate this requirement and permit account opening, and general transactions.)

Several group discussions centered on when, precisely, an account is considered open. With loans, for example, the issue might hinge on when it is approved versus when the funds are released. For business accounts, the question might be on when the account is created versus when deposits are first made.

Attendees also discussed establishing risk-based procedures to verify the identity of each beneficial owner "to the extent reasonable and practicable." There were split opinions on what that will mean in practice. One attendee's institution plans to verify by phone. The employees will attest they obtained the information, which the institution will consider a verification document.

Takeaways

- There is widespread agreement that principles of beneficial ownership collection for new accounts be documented in policies and procedures, but views differ on operational fine points such as relying on previously collected client information
- Approaches vary on opening accounts without full ownership identification and verification, with some financial institutions (FIs) allowing a window to subsequently collect the information
- Many attendees felt the definition of a new account can be a gray area, such as existing clients who open multiple accounts in the regular course of business.

A Heartbeat Away? Drilling Down, Certification and Appendix A

The CDD Final Rule will impact onboarding, but some attendees were unclear on how the new rule might affect client screening.

Virtually all attendees routinely conduct OFAC screening on beneficial owners, and that will continue under the new rule.

However, many do not routinely perform 314(a) screenings and attendees split on whether they would do so once the new rule takes effect. (Some said 314(a) screenings might take place in other contexts, such as part of risk-based reviews.)

Attendees expressed confusion about what the regulation requires in terms of reporting a 314(a) match with a beneficial owner.

At many tables, there were discussions of "drilling down" in cases where beneficial ownership could not be readily identified. Most attendees said they intend "to drill down to a heartbeat." However, some acknowledged that this could prove difficult in practice.

There was divergence among attendees on whether, and to what extent, banks could rely on representations made by the person opening the account, or whether they will be expected to investigate to find a "beating heart."

Others said drilling down efforts must be supported institutionally with formalized escalation processes. One approach might be to work in conjunction with existing AML steering committees, and institutions might consider creating a separate beneficial ownership escalation committee. Again, staffing is a realistic concern.

Views diverged on whether to collect information on intermediary entities while drilling down to natural persons. Some said yes, others no, and others said only with high-risk clients. A key component of drilling down is documenting investigative steps taken.

Views were mixed on whether to use the certification form attached to the rule's Appendix A. Some institutions will utilize it and others will create something in-house. Some FI's will ask the person opening the account to fill in Appendix A; others will complete it and ask the customer to certify the information. Some attendees are considering added information such as citizenship and possible PEP connections.

Takeaways

- OFAC screening is regularly conducted on beneficial owners, but 314(a) scans are less frequent, and there is some confusion about reporting 314(a) matches
- Institutions plan to drill down to "a beating heart" but some are uncertain how much they may rely on representations of the person opening the account and if/when they must investigate independently
- Appendix A will often be used, and sometimes integrated into internal systems, although others plan to create their own disclosure forms in-house

Tech Tools: Developing IT to Address New Systemic Needs

The CDD Final Rule creates new challenges in terms of technology and data management, which many attendees said are unresolved.

There was widespread agreement that vendors are generally not yet providing products tailored for the CDD Final Rule. While most attendees have automated processes to assist compliance workflow, they are still evaluating whether these systems can be adapted to ensure beneficial ownership information flows through filters such as screening for currency transaction reporting (CTR) aggregations and sanctions risks.

Several attendees are in the process of engaging with vendors, to jointly develop systems, timetables and budgets. But several said vendors do not seem to have a firm grasp of the rule and its requirements. The ultimate liability falls with the FI, so proper and intensive due diligence is a must. If you disagree with your vendor, you may have to ask them to change their process or handle the issue in another manner.

Many believe the process should begin with a gap analysis, to determine the performance of current systems versus the desired performance after the rule is implemented. This gap analysis, they said, will enable them to craft systems to better serve their needs, and identify expected costs and hiring needs.

There were varied approaches to how beneficial ownership data will be stored. For smaller institutions, it will often conform to current document management systems. However, as institutions increase in size, there was a greater likelihood of creating an internal data warehouse dedicated to beneficial ownership information. Some said managing that data may require revisiting policies on client privacy protection.

Takeaways

- Technology is crucial to successfully implementing the CDD Final Rule, but many vendors are not yet offering products specifically tailored to this regulation
- Institutions should consider conducting a gap analysis to identify the rule's expected impact on workflows and pinpoint expected costs such as staffing needs
- Data management plans include using existing document handling systems and dedicated internal warehouses, and client privacy protections are a concern.

Spread the Word: Conducting Training from the Front Line to the C-Suite

Attendees said one of their top challenges is generating awareness of the CDD Final Rule internally and incorporating it into the existing culture of compliance.

There was a consensus that buy-in by senior management is vital. This support should include funding for IT and staffing (see above.) Equally important, senior management must clearly signal that the rule is an enterprise-wide responsibility.

Many attendees have formed—or plan to form—implementation teams, comprising various internal constituencies and relevant third parties such as vendors. The goal, as one attendee put it, is to "socialize" the rule, or build broad awareness of it.

Some implementation teams might develop a decision tree, with clearly defined responsibilities and deadlines for each team member.

Effective staff training, attendees said, requires assessing the rule's impacts on specific lines of business (LOBs) because the impact will vary among units. This will allow for tailored training that addresses discrete risks of each LOB. Attendees plan to use computer-based training as well as targeted in-person sessions, particularly for senior management.

For front-line staff, most attendees plan a "train the trainer" approach, or training team leaders who then school fellow staffers.

One potential hurdle is that few standardized training materials are available at present. Some attendees plan to develop such materials internally; others may look for third-party instructors to ensure training deadlines are met.

A number of attendees said training for front-line workers should include explaining the rule itself and defining its obligations. Staff will also be trained to handle situations where information is either incomplete or inaccurate.

Many institutions will utilize scenario training, which simulates real-life cases and provides appropriate responses. As one attendee put it, however, there are almost certainly unknown scenarios that will arise post-implementation.

There was discussion, though no consensus, on whether to incentivize employees by methods such as making CDD Final Rule compliance a component of performance reviews, though some plan to reference the rule in job descriptions.

Due to the newness of the rule for both institutions and examiners, some attendees plan to regularly document and discuss their strategies with examiners. They will outline the steps they are taking, and the anticipated benefits. This documentation should enhance project analysis during implementation and potentially reveal systemic weaknesses.

Takeaways

- Compliance personnel must socialize the rule across the institution, but successful implementation requires buy-in from senior management and training front-line workers
- The newness of the rule calls for regularly communicating with examiners to ensure supervisory expectations and imperatives are addressed
- Training must be tailored for the unique needs of various business lines and the discrete risks of various products and services

Free and Clear? Tips on Managing Exclusions and Exemptions

The CDD Final Rule includes a number of exclusions and exemptions. Exclusions are for certain types of entities, such as regulated financial institutions and publicly traded companies. Trusts are also excluded (except for statutory trusts created by a filing with a secretary of state or similar office). Nonprofits that have filed organizational documents with appropriate state authorities are subject only to the control prong.

Certain types of accounts are exempted. An example is an account financing insurance premiums, where payments are remitted directly to an insurer or broker.

For attendees, a key issue, in some cases, is verifying eligibility.

In many cases, eligibility documentation will be provided by the client. Some institutions are developing drop-down options in new account applications that ask why the applicant is eligible. Opinions were mixed on requiring clients to certify eligibility on a form. Some felt exclusion forms should be required for new accounts. Some will make a risk-based decision.

Others said gray areas remain. For instance, equipment financing is exempted if it involves direct payment from the bank to the vendor or lessor. But "equipment" is not specifically defined; whether it applies to things such as automobiles used for business is unclear.

Takeaways

- Institutions should train staff on available exemptions and exclusions and incorporate eligibility determination into account opening processes
- Institutions must be aware of potential gray areas involving exemptions, such as transactions involving certain types of equipment financing and leasing
- Although clients may be the primary source of exclusion certification, additional steps may be advisable depending on the client's risk profile

A Clear Message: Managing Client Communication and the Customer Experience

Many attendees said a challenge posed by the CDD Final Rule is communicating it to clients and explaining how it may affect them.

Attendees want to make the customer experience pleasant and understandable. Several plan to emphasize the rule is a regulatory requirement, not a unilateral decision by the institution. Nevertheless, some feared clients might object or shop for an institution with less stringent policies.

There was a general consensus that communication will require repeat messaging, on different communication platforms. Some plan a separate mailer outlining the rule and its requirements. The letter may be included in account statements.

Others said letters might prove inadequate, and should be supplemented with branch signage and a social media or online outreach effort. A Frequently Asked Questions (FAQ) posted on bank websites would also be helpful.

There was a hope expressed by some for FinCEN to create a brochure as well, similar to one it produced regarding CTR requirements.

In addition, banks must provide talking points and FAQs to relationship managers and other personnel to ensure accurate responses to client queries.

Takeaways

- Communication with clients is essential and should be conducted on an ongoing basis utilizing multiple messaging platforms
- Creating informational tools such as FAQs for use by relationship managers and front-line personnel will support consistent messaging to clients
- The communication should emphasize the new rule is a regulatory requirement not an elective institutional policy

All Systems Go: Shared Ideas on Launching (and Completing) Implementation

With the CDD Final Rule deadline of May 11, 2018, attendees debated implementation strategies that minimize disruption to operations and clients.

The majority of attendees intend to roll out their new regime in the first quarter of 2018, although a handful plan to initiate it in the fourth quarter of 2017.

Most are doing so incrementally. Many plan to design new workflow processes to attain standardized compliance practices across the institution. Initially, they will operationalize new workflows with pilot projects or beta testing in conjunction with vendors. These small-scale tests will then be subjected to quality control reviews to spot systemic deficiencies. One specific area of interest will be identifying where increased automation might enhance operational efficiencies.

One group said the implementation process should focus on five types of risk: compliance risk; operational risks such as proper resource allocation; technology risks including data flow and record retention; strategic risks such as unpleasant customer experience; and reputational/legal risks.

Documentation of the testing process should be thorough, and senior management and the project management team must be briefed on the progress. Decisions to alter the original model, and why, should also be documented.

The estimated amount of time for this initial phase varied, though several believed it would take at least four months.

Following that, most plan a gradual rollout, such as by LOB. This will mitigate strains on available training resources.

For long-term quality control, planned approaches varied. Smaller institutions tended to favor random sampling of new account openings; larger ones anticipated moving toward 100% quality control review for high-risk clients.

Takeaways

- Institutions should reserve several months for implementing the rule, beginning with controlled testing and pilot projects
- Early tests should be reviewed to identify areas needing enhancement, while documenting all subsequent model alterations and the reasons for them
- System rollout will be incremental in most cases, to address unique issues facing different LOBs and ensure rational allocation of training and IT resources

Review and Conclusions

The day concluded with presentation of findings by facilitators and a review and analysis by Rick Small, ACAMS advisory board chairman and executive vice president and director, Financial Crimes Program at BB&T.

Mr. Small outlined the rule's four core elements of CDD. They are (1) customer identification and verification; (2) beneficial ownership identification and verification; (3) understanding the nature and purpose of customer relationships to develop a customer risk profile; and (4) ongoing monitoring for reporting suspicious transactions and, on a risk basis, maintaining and updating customer information.

The first is already an AML program requirement. The third and fourth are implicitly required to comply with suspicious activity reporting requirements. The second is required under the new rule.

AML program requirements are being amended to explicitly include risk-based procedures for ongoing CDD, including understanding the nature and purpose of customer relationships for purposes of developing a risk profile. A risk profile refers to information gathered at account opening, to be used as a baseline against which customer activity is assessed for suspicious activity reporting. The profile may, but need not, include a system of risk ratings or customer categories.

The AML program amendments also include conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, update client information, including beneficial ownership.

When, in the course of normal monitoring, a financial institution detects information relevant to assessing client risk, including possible changes in beneficial ownership, it must update customer information including beneficial ownership. There is not a categorical requirement to update client information on a continuous or periodic basis. Updating is to be event-driven.

For identifying and verifying customers, current processes need not change. Current CIP requirements meet CDD standards.

However, understanding the nature and purpose of customer relationships may require evaluating current risk rating and enhanced due diligence (EDD) systems to ensure they meet minimum standards. A key issue is regulatory expectations for what information should be collected at account opening.

Existing ongoing monitoring processes and procedures should suffice in terms of maintaining and updating customer information, and identifying and reporting suspicious transactions. But institutions must adhere to regulatory expectations for "refreshing" beneficial ownership information.

Takeaways

- AML program requirements are being amended to explicitly include risk-based procedures for conducting ongoing CDD, to include understanding the nature and purpose of the customer relationship for purposes of developing a risk profile
- A risk profile refers to information gathered at account opening and should be used as a baseline against which customer activity is assessed for suspicious activity reporting
- There is no categorical requirement to update customer information, including beneficial ownership, on a continuous or periodic basis, but rather the updating requirement is event-driven and occurs as a result of normal monitoring

Acknowledgements

Moderators for the ACAMS Special Forum: Mastering the CDD Final Rule—A Roadmap to Successful Implementation were John Byrne, Esq., CAMS, executive vice president of ACAMS, and Kieran Beer, CAMS, editor-in-chief of ACAMS moneylaundering.com.

ACAMS expresses sincere and deep gratitude to the forum's facilitators. In alphabetical order:

Megan D. Hodge, CAMS, executive compliance director and BSA/AML officer, Ally Financial;

Lauren Kohr, CAMS-FCI, chief risk officer and BSA officer, Old Dominion National Bank;

Megan Nelson, senior vice president and manager of Financial Crimes, Governance and Risk Assessments, BB&T;

Anna M. Rentschler, CAMS, vice president and BSA officer, Central Bancompany;

Tyler Reynolds, CAMS, senior vice president and senior director of enterprise financial crimes compliance, US Bank;

Rick Small, CAMS, executive vice president and director, Financial Crimes Program, BB&T and chairman of the ACAMS Advisory Board;

Joe Soniat, CAMS-FCI, vice president and BSA/AML officer, Union Bank and Trust;

Daniel P. Stipano, partner, Buckley Sandler;

Chuck Taylor, CAMS, senior vice president and BSA officer, City National Bank;

Susan Tuccillo, CAMS, senior vice president and head of compliance, Nordea Bank AB (New York branch)

This paper was written by Gregg Fields, CAMS, senior copywriter of ACAMS, based on his reporting from the forum and notes submitted by the facilitators.

Additional Resources

The following link is to FinCEN's Notice of Proposed Rulemaking on Customer Due Diligence Requirements for Financial Institutions, posted Aug. 4, 2014

https://www.regulations.gov/document?D=FINCEN-2014-0001-0001

The following link is to FinCEN's Preliminary Regulatory Impact Assessment for the CDD Final Rule, posted December 2015

https://www.fincen.gov/sites/default/files/shared/CDD_RIA.pdf

The following link is to FinCEN's issuance of the final rule, posted May 11, 2016

https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions

The following link is to an FAQ on the rule posted by FinCEN on July 19, 2016

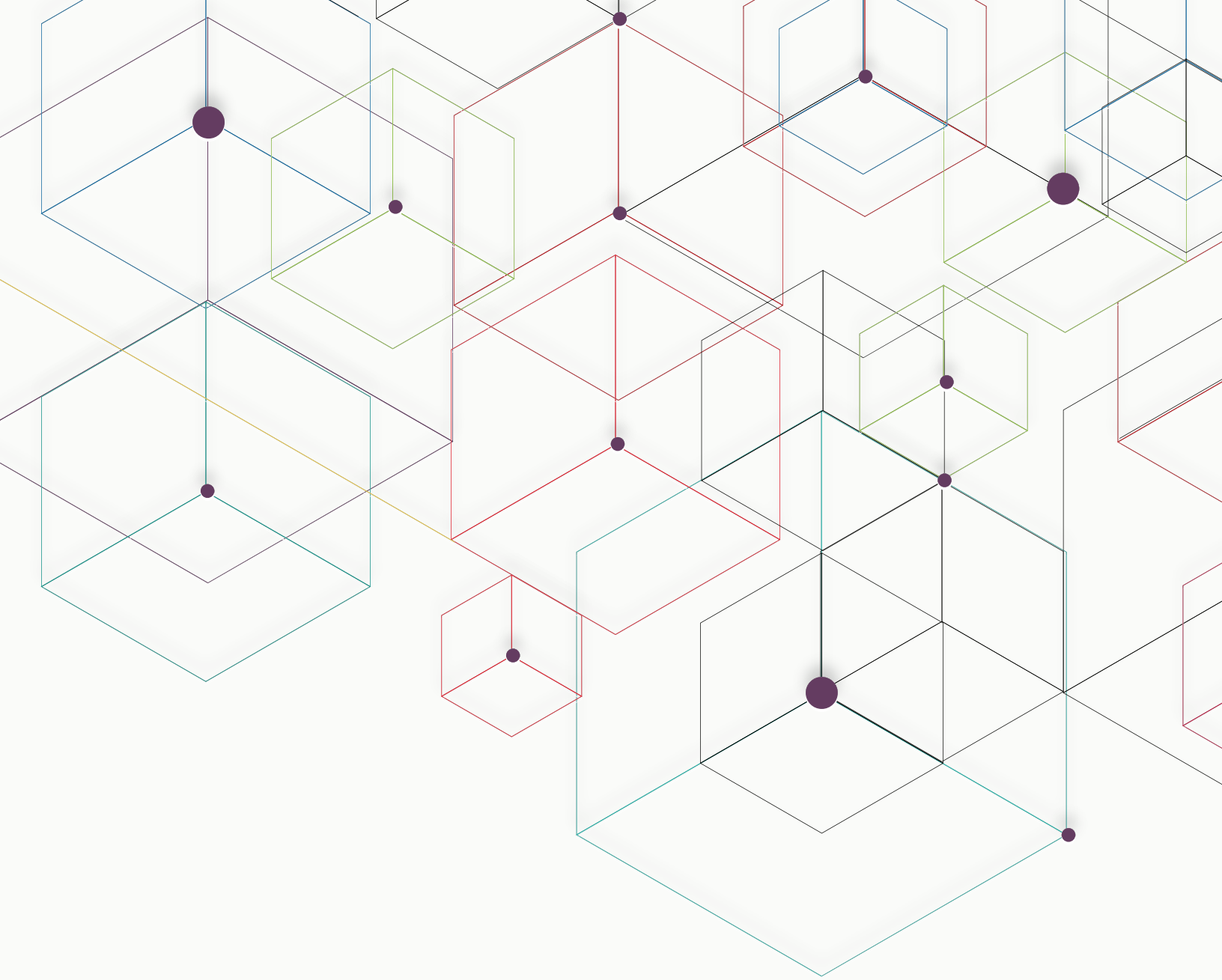
https://www.fincen.gov/sites/default/files/2016-09/FAQs_for_CDD_Final_Rule_%287_15_16%29.pdf

The following link is to a free ACAMS webinar, The CDD Final Rule: Responding Effectively to Implementation Hurdles, conducted on May 12, 2017

http://www.acams.org/webinar-2018-cdd-final-rule/

"ACAMS KYC CDD - Intermediate" certificate course builds research skills for complex cases, shell companies, and ultimate beneficial owners.

http://www.acams.org/kyc-cdd-intermediate-training/



ACAMS® | Advancing Financial Crime Professionals Worldwide®