Best Practices in KYC for Financial Institutions

November 2012

alacra
New York ▪ London

Alacra provides workflow solutions and reference data products to financial institutions.

Alacra Compliance Enterprise is a workflow tool for client onboarding that incorporates content from disparate sources. It delivers a cost-effective, consistent process for Customer Identification, Know Your Customer and Enhanced Due Diligence that meets all regulatory requirements.

Alacra Counterparty Intelligence provides accurate and enriched reference data on financial institutions' clients and counterparties. Using proprietary matching software and a global research team we offer a suite data alignment, entity identifier mapping and risk monitoring solutions.

For 16 years Alacra has partnered with clients and business information publishers to build innovative, content-rich products that are now in use at over 250 banks, insurance companies, professional service firms and corporations.

To learn more, call us:

888.333.0820 (Toll Free)

212.363.9620 (US)

44.020.3059.5765 (UK)

Introduction

Alacra has been delivering Compliance Workflow solutions to financial institutions since 2005. Our sales and implementation process usually involves many client meetings. As we're working out the configuration with the client, the question we are most often asked is, "What are other banks doing to solve these challenges?"

That's a tough question for us to answer for three reasons. First, we have confidentiality and non-disclosure agreements in place with all our clients so we can't say anything about a specific firm. Second, our clients are spread out geographically and are therefore subject to different regulatory regimes. That influences what they do and how they do it. Finally, processes and procedures for KYC vary widely not only from bank to bank but within different departments in a single bank.

To help answer the question, "What are other banks doing?" we have put together this white paper, which ties together various regulations with best practices in three key areas of the Know-Your-Customer process. The three areas we focus on are:

1. Customer Identification
2. Customer Due Diligence
    a. Risk-based Approach
    b. Sanctions Lists, PEPs and Database Checks
    c. Beneficial Ownership
3. Ongoing Monitoring

We have reviewed much of the relevant regulation from both government regulators and industry trade groups and have highlighted key segments of the regulations at the beginning of each section. Our focus has been on regulations related specifically to anti-money laundering and know-your-customer but we have also included information on FCPA, UK Anti-Bribery and FATCA, as there is an important KYC component to each. We then describe what we believe are the best practices in each area based on our work with our clients and prospects.

Throughout this document we repeatedly refer to the KYC process. We have found that firms that focus on improving each part of the process usually exhibit more of the best practices we have described herein and that these firms were much less likely to experience difficult regulatory audits.

Customer Identification–Regulatory Highlights

Every regulatory framework that oversees a financial institution interacting with a customer emphasizes customer identification as a critical first-step in anti-money laundering compliance.

FinCEN (Financial Crimes Enforcement Network, US Department of Treasury): In the United States, FinCEN regulates the customer identification procedures (a.k.a. "know your customer rules") at banks. A bank's CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. It is critical that each bank develop procedures to account for all relevant risks including those presented

Copyright 2012 © Alacra Inc.

by the types of accounts maintained by the bank, the various methods of opening accounts provided, the type of identifying information available, and the bank's size, location, and type of business or customer base. Thus, specific minimum requirements in the rule, such as the four basic types of information to be obtained from each customer, should be supplemented by risk-based verification procedures, where appropriate, to ensure that the bank has a reasonable belief that it knows each customer's identity.

The Agencies note that the CIP, while important, is only one part of a bank's BSA/AML compliance program. Adequate implementation of a CIP, standing alone, will not be sufficient to meet a bank's other obligations under the BSA, regulations promulgated by its primary Federal regulator, such as Suspicious Activity Reporting requirements, or regulations promulgated by the Office of Foreign Assets Control.[1]

JMLSG (Joint Money Laundering Steering Group): "The firm identifies the customer by obtaining a range of information about him. The verification of the identity consists of the firm verifying some of the information against documents, data or information obtained from a reliable and independent source."[2]

FATCA (Foreign Account Tax Compliance Act, US Department of Treasury, Internal Revenue Service): "Requires a financial institution to report indicia of US status: US citizenship or lawful permanent resident (green card) status; a US birthplace; a US residence address or a US correspondence address; standing instructions to transfer funds to an account maintained in the US; an "in care of" address or a "hold mail" address that is the sole address with respect to the customer; a power of attorney or signatory authority granted to a person with a US address."

Customer Identification–Best Practices

In Stephen Covey's "The Seven Habits of Highly Effective People," habit number two is "Begin with the end in mind." Customer Identification is the start of the KYC process. Basically, a thorough customer identification procedure can set the stage for best practices throughout the entire onboarding process. One variable is how much data is the front desk or the relationship manager responsible for acquiring? Weaker firms in terms of process required only the customer's name. Stronger, process oriented firms had relationship managers getting address and other basic documentation from the customer, which was then verified by the due diligence team.

Our experience with "how customer identification is achieved" varies widely from firm to firm and occasionally from department to department. In some cases customer identification is handled with aplomb by the relationship managers dealing with the customer, in other cases customer identification responsibilities are delegated to the customer due diligence team. When customer identification is given to the Customer Due Diligence (CDD) team, the method of communication between the relationship manager and the CDD team is where a best practice can most effectively be deployed.

We found three ways this communication is completed:

- Unstructured—essentially no process.

Copyright 2012 © Alacra Inc.

- Structured—through a request form or email that is used consistently.
- System-to-system—electronic communication from a relationship management system to a KYC/onboarding system.

As a general rule, financial institutions with unsystematic data entry mechanisms also had an overall poor KYC process. Therefore, a crucial "best practice" recommendation is to start the process in a robust manner. Without a clean and precise data entry process, it is practically impossible for a financial company to create an accurate onboarding audit trail (which will be discussed later in greater detail). Another potential risk is that the on-boarding process from initiation to completion includes many expensive, manual processes that can take days or weeks to finalize.

Often, an unsystematic process requires scanning or re-keying information into multiple internal and external back-office systems, which increases the risk of inaccuracies and spelling mistakes. To address these issues, companies should invest in an electronic data system that enables staff to key information once and then have duplicate data auto-populated into other areas of the same form or into other forms.

This will become even more critical as regulations such as FATCA become effective as the customer identification process becomes more complex, with various indicia being required to determine if the client falls under the FATCA regime. There are likely to be regulations that are similar to FATCA in other jurisdictions in coming years.

Customer Due Diligence–Regulatory Highlights

The CDD area is where Alacra has the most experience so we have taken a more detailed look at the CDD process by breaking it up into three sections: risk-based approach; sanctions lists, PEPs and database checks; and beneficial ownership. Directly below are excerpts that reveal the vagueness of regulatory instructions for CDD and KYC; we will have other more specific regulatory examples in the sections that follow.

FFIEC/BSA (Federal Financial Institutions Examination Council/Bank Secrecy Act): "The objective of CDD should be to enable the bank to predict with relative certainty the types of transactions in which a customer is likely to engage. These processes assist the bank in determining when transactions are potentially suspicious. The concept of CDD begins with verifying the customer's identity and assessing the risks associated with that customer. Processes should also include enhanced CDD for higher-risk customers and ongoing due diligence of the customer base."[4]

FSA (Financial Services Authority, UK): "Although there are no specific legal or regulatory KYC (as opposed to simple identification) requirements, high-level obligations in the Money Laundering Regulations and the FSA Handbook require a firm to counter the risk of money laundering."[5]

FATF (Financial Action Task Force): "Financial institutions should be required to undertake customer due diligence when: a) establishing business relations; b) carrying out occasional transactions over a designated threshold; c) there is a suspicion of money

Copyright 2012 © Alacra Inc.

laundering or terrorist financing; d) the financial institution has doubts about the veracity or adequacy of previously obtained customer data. CCD includes identifying and verifying the customer's identity; identifying the beneficial owner; understanding the business relationship; conducting ongoing due diligence on the business relationship."[6]

Customer Due Diligence–Best Practices

While only the language from the FSA says, "there are no specific legal or regulatory KYC requirements," the truth is that there are few KYC process mandates in any of the jurisdictions in which Alacra has clients. This has led to a wide range of practices across firms and across department within firms. Whereas the stronger firms have robust practices in place for each of the next remaining sections of this paper, we've seen weak customer identification followed by a handful of Google searches and some paper files constituting an entire KYC effort.

Here are a few overall best practices before we get into more specific customer due diligence areas. These might seem obvious, but a surprising number of financial institutions do not have these practices in place.

1. Anywhere you can create a process you should create a process. In a regulatory audit, having onboarding professionals conducting due diligence in a consistent fashion will indicate the organization takes KYC seriously and has trained employees on how to do their jobs effectively.

2. Have an audit trail for each investigation. This will prove that the onboarding process was adhered to for each and every investigation and that there was no material adverse data as of the investigation date.

3. Have a "do not do business with" database. This will eliminate unnecessary work and indicate to regulators that you're keeping track of bad guys.

4. Have a database of entities that have been successfully onboarded. This can save significant amount of resource when an existing, already vetted customer wants to do more or different business with your institution. This can also help define your refresh schedule and reduce the number of times you need to go back to the customer for more information.

5. Don't fall behind on your refresh schedule.

Risk-based Approach–Regulatory Highlights

"Risk-based approach" is a phrase used in many domains, from pharmaceutical manufacturing practices to auditing, to testing internal controls, to combating money laundering and terrorist financing. The AML regulations are consistent in saying a risk-based approach should be deployed; our best practices that follow explain how some financial institutions get this done.

Copyright 2012 © Alacra Inc.

BSA (Bank Secrecy Act): "Under the BSA and its implementing regulations, and, with respect to banks, parallel requirements of the Federal bank regulators, banks, securities broker-dealers, and certain other "financial institutions" are required to implement risk-based anti-money laundering ("AML") programs to prevent and detect money laundering and terrorist financing and to comply with a labyrinth of BSA/AML laws, regulations, and regulatory guidance."[7]

FCPA (Foreign Corrupt Practices Act): "We recommend companies follow a risk-based approach: focus on the nature of relationships with their distributors. Determine which distributors are the most likely to qualify as agents, for whose acts the company can be held responsible. Once a company segregates the high-risk distributors that likely qualify as agents and potentially subject the company to FCPA liability from mere resellers that pose little FCPA risk, FCPA compliance procedures can be tailored appropriately. Distributors that qualify as ''agents'' and also pose FCPA risk, full FCPA due diligence, certifications, training, and contract language are imperative."[8]

FSA: "Firms must put in place adequate and risk-sensitive AML policies and procedures. This means that firms have to identify and assess their money laundering risk and put in place systems and controls adequately to manage and mitigate this risk. Firms who apply a risk-based approach to AML will focus AML resources where they will have the biggest impact. The risk-based approach means a focus on outputs. Firms must have in place policies and procedures in relation to customer due diligence and monitoring, among others, but neither the law nor our rules prescribe in detail how firms have to do this. Firms' practices will vary depending on the nature of the money-laundering risks they face and the type of products they sell."[9]

Risk-based Approach–Best Practices

Most firms we have spoken to have a set of basic rules in place that are used to assign a risk rating to an entity. These are usually based on geography of the customer, type of customer, kind of business the customer wants to do with the bank and the appropriateness of that business to the customer. In addition, some firms will check to see if an entity has any listed securities and will see if the entity is regulated by an "approved" regulator. The list of "approved" regulators varies from firm to firm. For higher risk entities or entities that have affiliated PEPs, some firms have a four-eye review process, where a peer must review the work of the KYC investigator. Some firms conduct a four-eye review on all investigations because they want a second set of eyes confirming an entity is low-risk. More difficult or high-risk investigations are often conducted by more seasoned analysts.

Our observations reveal that the degree to which financial institutions deploy a risk-based approach depends on three factors: 1) communication between relationship managers and the KYC team; 2) size of business the customer intends to do with the financial institution and 3) the level of "process" employed by the KYC team.

The more formal the communication is between relationship managers and the KYC team, the more likely that critical information about the applicant will be complete. When the KYC team understands the type of business the customer wants to conduct, from which

Copyright 2012 © Alacra Inc.

geography and in what size or volume, they can conduct the appropriate level of due diligence. Lack of such communication often results in many customers being onboarded in the same way, often with less rigorous diligence.

In the case of size of business, a risk-based approach is simply the deployment of common sense. In the commercial banks we observed there was a strong correlation between the level of due diligence and the size of the loan applied for, both to combat money laundering as well as to reduce credit risk.

Beneficial Ownership–Regulatory Highlights

Patriot Act (USA Patriot Act): The final rules similarly provide that, based on a financial institution's risk assessment of a new account opened by a customer that is not an individual, a financial institution may need to take additional steps to verify the identity of the customer by seeking information about individuals with ownership control over the account, including signatories.[10]

FinCEN: On Feb. 29, 2012, FinCEN issued an ANPR (Advance Notice of Proposed Rulemaking) seeking comments on a proposed CDD regulation that would explicitly require covered financial institutions to institute defined programs to identify the real or beneficial ownership of accountholders. FinCEN noted in its ANPR that there currently are two limited circumstances (concerning private bank accounts and correspondent accounts) in which financial institutions are expressly required to obtain beneficial ownership information, and that it is considering expanding the explicit requirement to obtain beneficial ownership information to all customers.[11]

FATCA: The Internal Revenue Service has published a draft of Form W-8BEN-E, which overseas entities must use to certify beneficial ownership status for US withholding tax purposes under the Foreign Account Tax Compliance Act. Depending on which of the 22 different descriptions that they correspond to in Part 1, which deals with the identification of the beneficial owner, entities are directed to different sections of the 25-part document.[12]

FATF: "Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer."[13]

Beneficial Ownership–Best Practices

Identifying beneficial owners is the most difficult part of the onboarding process. In the seven years Alacra has been providing compliance solutions, we have seen the beneficial ownership requirements increase dramatically. Early on, only owners of 50% or greater needed to be identified. Then for several years most institutions were collecting information on 25% and above owners. Now many firms are interpreting the FATCA requirement to be owners of 10% and above. Financial institutions are revolting against FinCEN's recently proposed plans to make beneficial ownership verification even more difficult. Once you have established who the beneficial owners are (and in many cases the officers and

Copyright 2012 © Alacra Inc.

directors) each individual (often referred to as a related entity) must have a PEP check, sanctions check and adverse news search run on them.

In terms of acquiring beneficial ownership information we've seen a wide range of techniques and databases used. One flaw we've seen in some banks is that they conduct entity due diligence separately from their beneficial owner due diligence. Our best practice recommendation is to keep the related entities—officers, directors and beneficial owners—together in the same investigation with the customer or counterparty being vetted.

Sanctions Lists, PEPs and Database Checks–Regulatory Highlights

Nowhere in the regulations are financial institutions instructed to use a proprietary database or conduct a proscribed level of research when onboarding a new customer or counterparty. Yet this is where the bulk of the money is spent, in database costs, workflow tools and investigative labor. As this is where the money is, and this is where Alacra has the most direct experience, we have provided a number of detailed best practices with regard to the research component of KYC.

Patriot Act: Section 326 says all banks must have a written CIP that describes client entity verification and determine whether the name of the new customer appears on any government list of known or suspected terrorists or terrorist organizations. Banks should take all reasonable steps to ensure that they do not knowingly or unwittingly assist in hiding or moving the proceeds of corruption by senior foreign political figures, their families, and their associates. Because the risks presented by PEPs will vary by customer, product/service, country, and industry, identifying, monitoring, and designing controls for these accounts and transactions should be risk-based.[14]

FSA: "Firms need to ensure that prospective and existing customers are assessed for being potential PEPS, either under the definition set out in the Money Laundering Regulations ("MLR's") or by reference to a wider definition…In this regard it is important to remember that PEPs include those who are family members or "known associates" of PEPs."[15]

FATF: "Financial institutions should be required, in relation to politically exposed persons (PEPs) (whether as customer or beneficial owner) in addition to performing normal CDD measures to: a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person; b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships; c) take reasonable measures to establish the source of wealth and source of funds; and d) conduct enhanced ongoing monitoring of the business relationship."[16]

Copyright 2012 © Alacra Inc.

Sanctions Lists, PEPs and Database Checks–Best Practices

Again, communication is critical. Those firms that utilized electronic communication from the relationship manager to the onboarding team had better processes overall. In some cases searches of various databases (sanctions lists, PEPs, adverse news) were run automatically on the verified customer name from the relationship management system. This eliminated re-keying of data, which is a surprisingly costly effort and contributes significantly to operational risk. One firm admitted, "It's not that unusual for us to vet the wrong person."

A question we often get is, "What do other banks do in terms of database searches. Answers vary widely for these reasons:

1. More searching/researching creates higher costs and everyone wants to reduce costs.

2. Similarly, more searching/researching will generate more false positives, which also leads to higher costs and everyone wants to reduce costs.

3. No one will readily admit the amount of KYC due diligence they are conducting to actually prevent money laundering and terrorist financing and how much KYC they are doing to meet the vague regulatory requirements of the jurisdictions in which their companies operate. In other words, they are covering their backside.

At a minimum, all clients are searching sanction lists and adverse news.

Many firms search on the verified customer name as well as on a set of name variations and potential aliases using commercial software or an in-house system. Most firms also search their own "do not do business with" list that was a component of their research. In the US, commercial banks making significant loans often search legal databases for criminal record, liens, judgments and changes of address.

Ongoing Monitoring–Regulatory Highlights

BSA/Patriot Act: "As due diligence is an ongoing process, a bank should take measures to ensure account profiles are current and monitoring should be risk-based. Banks should consider whether risk profiles should be adjusted or suspicious activity reported when the activity is inconsistent with the profile."[17]

FinCEN: "Based on past efforts and ongoing industry and regulatory consultation and outreach, FinCEN believes that an effective CDD program includes conducting ongoing monitoring of the customer relationship and conducting additional CDD as appropriate, based on such monitoring and scrutiny, for the purposes of identifying and reporting suspicious activity."[18]

FATF: "Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the institutions knowledge of the customer, their business and risk profile, including, where necessary, the source of funds."[19]

Copyright 2012 © Alacra Inc.

Ongoing Monitoring–Best Practices

All the financial institutions we've worked with have deployed a transaction monitoring system that alerts the bank to suspicious activity. Sophisticated financial institutions have entities exhibiting unusual activity automatically sent to the due diligence team for review. This review results in the KYC information for that entity being updated.

Firms also monitor or refresh their customer and counterparty due diligence information on a regular schedule: high-risk entities every six months to a year; medium-risk entities every two years; low-risk entities every three years. Some larger banks monitor their customers much more closely, screening entities on a daily basis against commercial databases of Sanction List hits and adverse news.

Conclusions

We cannot emphasize enough the importance of process. There was a clear correlation between firms that were focused on process and those following "best practices." As we mentioned earlier in this paper, "Begin with the end in mind." The start of the process is critical to the entire endeavor and the start of the process is communication between the sales team and relationship managers and the KYC team. The more information gathered from the customer up front and the more clearly this information is communicated to the due diligence professionals, the more effective the onboarding team will be.

Firms displayed a wide range of techniques when conducting the actual due diligence. We have observed the use of different databases and different levels of care when investigators are doing their research. The "best practice" firms had trained their investigators to use consistent processes that were generally more rigorous than other firms. While all firms were conscious of cost and time spent on each investigation, those that deployed more rules, checklists and structure to the process were generally more cost-effective.

Finally, the firms that exhibited the most "best practices" tried to anticipate what a regulator would be looking for during an audit. They were concerned about audit trails for their investigations and having well-organized documentary evidence of their decisions to accept new customers.

Copyright 2012 © Alacra Inc.

Endnotes

[1] Guidance on Customer Identification Regulations Financial Crimes Enforcement Network; FAQs: Final CIP Rule; January 2004 http://www.fincen.gov/statutes_regs/guidance/html/finalciprule.html

[2] Joint Money Laundering Steering Group: Prevention of Money Laundering/Combating Terrorist Financing; November 2009 www.jmlsg.org.uk/downloads/Part_I_-_Post_Consultation.pdf

[3] Deloitte: FATCA Frequently Asked Questions September 2011; www.deloitte.com/...UnitedStates/.../us_tax_FATCA_FAQs_06...

[4] Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering InfoBase: Customer Due Diligence – Overview http://bit.ly/QfSDm1

[5] UK Financial Services Authority Discussion Paper 22: Reducing Money Laundering Risk; August 2003

[6] FATF Recommendation 5: Customer Due Diligence and Record-Keeping http://bit.ly/Lwo7Ap

[7] Gibson Dunn: Department of the Treasury Issues Bank Secrecy Act Advance Notice of Proposed Rulemaking Relating to Customer Due Diligence Requirements for Financial Institutions, April 2012; http://bit.ly/MEkQRR

[8] FCPA Professor, June 2012 http://www.fcpaprofessor.com/friday-roundup-42

[9] UK Financial Services Authority: The risk-based approach to anti-money laundering. http://www.fsa.gov.uk/about/what/financial_crime/money_laundering/approach

[10] Joint Release: Financial Crimes Enforcement Network, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, Securities and Exchange Commission – Guidance on Obtaining and Retaining Beneficial Ownership Information

[11] Payment Law Advisor: FinCEN Proposes Customer Due Diligence Requirement of Beneficial Ownership Identification to Enhance Federal Anti-Money Laundering and Counterterrorism Efforts, March 27, 2012 http://bit.ly/PL9PKe

[12] International Tax Review: Non-US entities get first sight of beneficial ownership form for FATCA, June 7, 2012 http://bit.ly/K2lge3

[13] FATF, op. cit.

[14] FFIEC Core Examination Overview and Procedures for Regulatory Requirements and Related Topics: Customer Identification Program – Overview http://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_011.htm

Copyright 2012 © Alacra Inc.

[15] Willkie Farr & Gallagher: Lessons To Be Learnt Regarding PEP's From Recent FSA Enforcement Action, May 29, 2012 http://bit.ly/O0DjYq

[16] UK Financial Services Authority: Banks' management of high money-laundering risk situations, June 2011 http://www.fsa.gov.uk/pubs/other/aml_final_report.pdf

[17] FFIEC Customer Due Diligence – Overview, op. cit.

[18] Schulte Roth & Zabel, FinCEN's ANPRM on Customer Due Diligence for Financial Institutions – Comments Due May 4 http://bit.ly/PLrRvV

[19] FATF, op. cit.

Copyright 2012 © Alacra Inc.