Sterling Talent Solutions

Employee, Client and Third Party Due Diligence

The Cost of Ineffective Monitoring Procedures

In Partnership With

compliance risk concepts

Introduction

Onboarding employees and registered representatives, and partnering with third parties, are keys to successfully growing your business. Firms, particularly those operating within the financial services industry, cannot overlook the importance of due diligence. Most firms have vetting procedures in place when selecting counterparty affiliations and vendors, or onboarding a new hire. Gathering background information to deem a person or organization as low risk is a great start, but in order to engage in truly effective due diligence practices, monitoring, oversight, and investigation must be ongoing. Having inadequate due diligence practices in place leaves an organization open to potential risks.

Operating with stale knowledge makes you vulnerable to increased operational and reputational risk, as well as potentially exposing client and firm resources and information to fraud and misappropriation.

Regulatory Priorities: Relevant Enforcements, Risk Alerts, and Findings

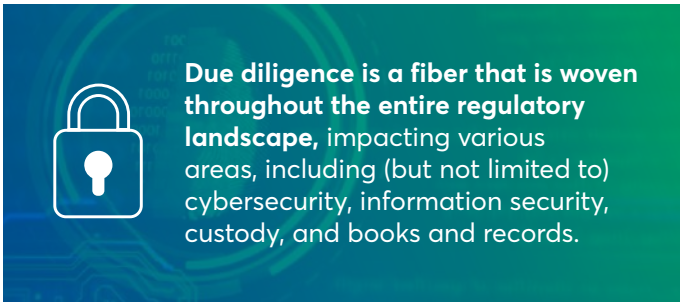
A central theme of FINRA's priorities for 2018 are the principles of investor protection and information security, both of which have a strong link to effective due diligence practices. Onboarding reps, engaging counterparties, and even bringing on clients can expose firm and client funds or private information to fraud, theft, or misappropriation in the absence of appropriate due diligence procedures. Firms must be able to not only believe their representatives are trustworthy and reputable, but continually verify information collected.

The same is true for counterparty relationships and clients. Organizations hoping to protect firm and client information will need to have stringent initial procedures coupled with ongoing reviews to ensure that the information they are working with to assess the risk profile of a particular counterparty or representative is current and complete.

Customer Due Diligence is also listed on the SEC's 2018 Exam Priorities List, and their Enforcement Actions Annual Report for 2017 included various cases that involved fraud or fraudulent activity. Elbit Imaging, Ltd, while not a financial company, is subject to SEC oversight under the Foreign Corrupt Practices Act of 1977. Elbit is an international holding company with several direct and indirect subsidiaries focused on, among other industries, real estate investment and development. Elbit exerts functional control over its indirect subsidiary, Plaza. Between 2007 and 2012, Elbit consolidated Plaza's financial statements into its own for the purposes of SEC reporting. In the order issued on the subject, the SEC noted that there was "no evidence to suggest that Plaza conducted any due diligence on the 2006 and 2011 consultant prior to entering into this agreement."

The total number of FCPA enforcement actions in 2017, many of which circle around the issue of due diligence, is the the second-highest total in the last decade following the highest number of actions in 2016. However, the average fine per company in 2017 was double that of 2016.

Regulatory inquests can be costly, both financially and time diverted to respond to request lists and host regulators onsite. The longer regulators stay onsite or in contact, the costlier it becomes for an organization. In addition, attorney fees and potential fines assessed in the event that issues are found compound the costs considerably. Once you add the potential for negative press, lost business, and client lawsuits, the cost of ineffective due diligence is substantial.



Employee and Registered Representative Due Diligence Best Practices

When onboarding new hires and registered representatives, firms should obtain and verify information such as an individual's education and work history, industry qualifications and certifications, criminal background checks and fingerprinting, credit checks, disciplinary information, and outside business activities, among other things. Verification is key, as simply obtaining this information is merely a first step.

Firms should use a reputable FCRA compliant background screening vendor or follow up and confirm all screening information that they receive from new hires and reps to ensure its accuracy. Firms may wish to consider implementing checklists or assembling a committee that periodically fleshes out any information that may impact an employee's risk profile with respect to the firm, a firm's desire to be associated with the individual, or customers' decision to invest. Due diligence procedures should be sufficient enough to unearth material "skeletons in the closet," and as the regulatory landscape evolves, so too does the information that firms need to collect.

Prehire due diligence is important, but as noted above, due diligence cannot be a "one and done" exercise if it is to be truly effective in detecting material changes or issues that could impact an investor or client. Firms should implement ongoing screening processes and disclosure monitoring that cover a nuanced array of areas outside business activities, political contributions donor lists and ongoing credit checks among other things. Firms need to be sure that they are capturing the whole picture when it comes to reps and employees by screening professional and financial information as well as continuing criminal background checks.

Data Collection

With respect to financial and professional information that firms need to collect from reps and employees, firms should develop comprehensive processes that will result in a detailed risk profile for each individual. Consider including questionnaires that pertain to outside business activities, personal brokerage accounts, political contributions, and social media and online footprint among other things. Many firms currently collect information on reps and employees via self-reporting regarding criminal actions, civil complaints, arbitration claims, liens, customer complaints, and regulatory sanctions.

Monitoring

Sole reliance on self-reporting, however, may not necessarily detect disclosable issues or protect a firm from respective consequences. Waiting for employees to disclose material events through monthly, quarterly, or annual certifications, or when running compliance checks, regardless of frequency, opens a firm to risk. A better, more proactive approach would include ongoing monitoring that can utilize comprehensive data and therefore screen for factors that traditional monitoring and self-reporting can miss. Firms may wish to consider partnering with a vendor that has access to data concerning criminal activity, liens and judgements (information which is no longer available via credit report), and regulatory sanctions and exclusions in order obtain the complete picture on a continual basis. Relying on reps and employees to self-report holds the potential for individuals to withhold material information, and even diligent annual or monthly compliance checks can typically only identify issues in arears or may miss key pieces of information entirely due to lack of resources.

Sterling
Talent Solutions

Verification

These initial processes and continued reviews, while time consuming, help firms generate the most clear and accurate information aimed at identifying real or perceived conflicts of interest, criminal activity, or regulatory issues. The next step in the process is to review and verify all of the information collected. Once verified, this information can help form the basis of assigning a risk rating to the individual and identifying areas that require additional inquest or research. Standardization of these processes can yield a "top down" approach to due diligence that eliminates the appearance of favoring or excusing certain employees or reps from these processes and will increase the likelihood that material issues are detected.

Beyond a customer's decision to invest, continually screening employees (pre and post hire) can mitigate the risk of exposing their funds or personal information to fraud, theft, or misappropriation, and, as such, exposure of the organization to lawsuits and subsequent negative publicity. From a regulatory perspective, having rigorous due diligence practices in place will satisfy exam teams and will potentially result in a quicker exam process with fewer findings in areas where due diligence is a factor.

Obtaining Information and Verifying Information

Allowing employees the option of self-reporting has various positive effects for the firm, including leaving employees with a sense that management trusts them. The process serves as a reminder of firm and regulatory expectations regarding conduct, and disclosing certain activities, as well. It does, however, leave a lot of potential gaps in the type and accuracy of information that a firm receives. A responsible firm will verify all information received via self-disclosure, but even this can still miss the mark in terms of capturing all material information. In addition, firms can spend countless hours on due diligence between initial and periodic data collection and verification, as well as escalating, investigating, and resolving any material issues that are detected throughout the process. Compounding the amount of time and resources dedicated to due diligence are the constantly evolving threats to be addressed and information that needs to be collected, coupled with changing regulation.

Organizations should carefully initially and continually review information from the following sources:

- Form U4
- OBA Certifications
- AML Checks
  - OFAC List
- DDQs
- Political Donor Lists
- Credit Reports
- Criminal Background Checks and Arrest Records
- Lien and Judgement Data
- Educational Institutions (Universities, CFA Institute, etc.)

Reviews should be varied and cover multitude of sources to obtain the most detailed profile of the intended counterparty, client, or representative.

Sterling
Talent Solutions

Client Due Diligence

Financial institutions should have AML procedures in place under FinCEN's new client due diligence (CDD) rule that went into effect on May 11, 2018. Such procedures, as with Counterparty and Firm Representative Due Diligence, protect the organization's reputation, limit exposure to litigation, fines or enforcement actions, and mitigate the risk of exposing client information and funds to fraud. A well-designed AML program should already include four of the five principles of the rule. Regulators currently expect that financial institutions obtain customer information at account inception, compose a customer risk profile, and use this profile during ongoing monitoring in order to identify potential red flags. Firms should focus on the five principles, as outlined below.

Identification and Verification

The rule requires that financial institutions gather information at account inception that will allow the identification of individuals who own and/or control legal entity customers. The identity of these individuals must be confirmed (government-issued IDs are generally acceptable forms of verification).

Ownership and Control

Ownership: Any individual(s) who directly or indirectly own(s) 25 percent or more of the equity interests in the legal entity must be identified. This means that up to four individuals may be identified; however, there may not be any individual identified (i.e., if no individual owns 25 percent or more).

Control: At least one individual **must** be identified who exercises significant managerial control over the legal entity customer (executive officers, senior managers, etc.) An individual identified under the ownership component noted above may also be identified in this area.

Exemptions

The rule contains various exclusions. The list of excluded legal entity types includes sole proprietors and unincorporated associations, as, typically, entities like this do not have a legal presence separate from the associated individual that could facilitate the concealment of their identity.

Certification Form

A certification form exists which outlines ultimate beneficial ownership (UBO) information that must be collected from each applicable legal entity customer; the use of this form is optional. Required UBO information may be obtained, per the rule, "by any other means that comply with the substantive requirements of this obligation… provided the individual certifies, to the best of the individual's knowledge, the accuracy of the information."

Updating UBO Information for Existing Customers

When a new or existing legal entity customer opens a new account, UBO information must be collected; however, there is no requirement to obtain or update UBO information for existing legal entity customers. Implementing a process to review and update this information should be considered a best practice.

Additionally, there is no requirement to update this information. FinCEN does expect that UBO information should be monitored via normal review procedures and updated if/when information is identified that is relevant to the customer's risk profile. Again, financial institutions should consider implementing a process to review and update this information on a regular basis.

Prior to the implementation of the CDD Final Rule, the ability for individuals to hide financial activity through anonymous ownership of legal entities was an obvious notch in the shield designed to prevent financial crime. In taking steps to gain a more complex profile of entity customers, financial institutions can take a risk-based approach to reducing the introduction of criminal or otherwise prohibited funds into the U.S. financial system.

The CDD Final Rule is a move toward increased financial transparency—a growing trend for regulatory bodies in 2018.

Third Party Due Diligence Best Practices

Standardization is key when counterparty due diligence is concerned. Committees formed for the purpose of creating and overseeing rep due diligence could expand their responsibilities to including developing similar procedures for counterparties, especially those that will have access to privileged information. Companies strive to implement repeatable procedures for due diligence that include drafting standard vendor and counterparty due diligence questionnaires, anti-money laundering (AML) checks, employee training, multi-level approval process that leverages Compliance Department, and adherence appropriate record keeping practices. Firms should use not the same but similar review practices, questionnaires, and recordkeeping practices for all applicable vendors and intermediaries to mitigate risk of missing material information from even seemingly innocuous vendors, counterparties, or relationships.

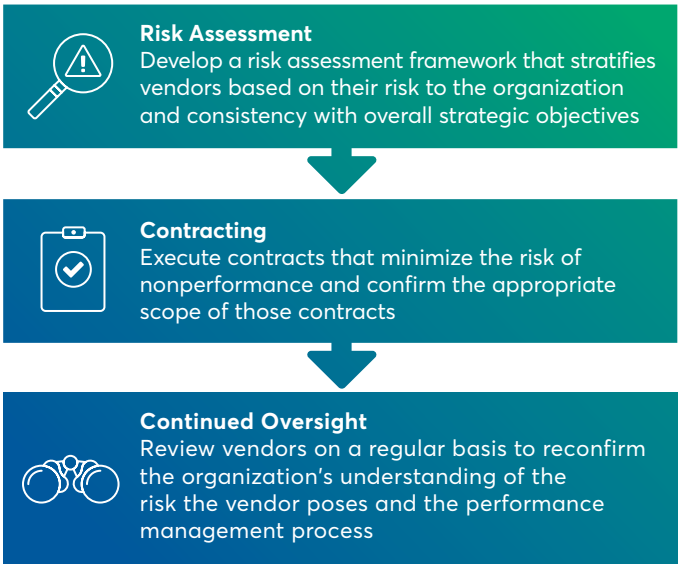
Firms should take a proactive, continual approach that reduces risk of delinquent records and catch material changes to information and situations. It's no longer the case that vendors can be approved and be permanently classified as low risk or "approved." Vendors and counterparties must be engaged and performing, and constantly reviewed by the firm to confirm that they still meet initial criteria, and that Due Diligence Questionnaires (DDQs) have been updated to account for any new concerns or regulatory implications. Reviews should be varied and cover a multitude of sources to obtain the most detailed profile of the intended counterparty.

As with rep and employee due diligence, considerable time and personnel resources need to be tapped in order to ensure that vendors and counterparties are subject to timely and appropriate screening, and that issues are investigated appropriately. Additional time and staff may need to be devoted to confirming that firm processes are up to date with current regulation and address ever-changing threats to firm and client reputation and operation.

Vendor Due Diligence

Prior to onboarding a new vendor, conduct a thorough assessment of the vendor's capability to deliver the services expected in line with the organizations expectations.

Key Activities In a Vendor Risk Management Program



Reputational and Operational Risks of Inadequate Due Diligence

While counterparty relationships are critical for the growth of an organization, they also expose it to various risks, including:

- Bribery and corruption
- Organized crime
- Money laundering
- Fraud

Non-compliance with anti-bribery and corruption and KYC/AML regulations, inadequate, or inappropriate due diligence processes can expose businesses to enforcement actions and fines, negative press and reputational damage, criminal penalties, sanctions against firms and covered individuals, and time wasted dealing with investigations and remediation. The cost of ineffective due diligence practices is real. Even firms engaging in conscientious data and disclosure monitoring for counterparties, reps, and even clients may be wasting time while also missing out on the ability to leverage a more complete, active data set.

In the long run, firms should be aiming for daily, continuous monitoring of varied, comprehensive data rather than relying on self-reporting due diligence models and quarterly or annual compliance reviews.

Conclusion

Having adequate onboarding procedures for reps, third parties, and even clients is not enough to avoid potential risks for the organization or its clients. Continual monitoring, risk assessment, and review of such information is imperative to protect assets and personally identifying information. The burden of time and resources that having truly effective "catch-all" due diligence can weigh heavy on an organization, so much so that compliance programs adopt policies that tick the minimum requirements meant to satisfy regulatory requirements but fail to identify issues in a timely, effective manner—if at all.

Sterling
Talent Solutions

The Sterling Talent Solutions Difference

Around the world, organizations of every size and across every industry rely on Sterling Talent Solutions to help them hire the best, most-qualified talent. Simpler is better when it comes to background screening and we help you cut through complexity so you can hire with confidence.

Here's what sets us apart from other background screening companies:

Outstanding Candidate Experience

A secure, mobile-responsive candidate portal provides simple anytime, anywhere access that engages your future employees throughout the hiring process. Our candidate portal not only offers the ability for candidates to complete and sign consent documents digitally, each touchpoint can be consistently branded to bolster your visual identity.

Speed and Efficiency

Sterling Talent Solutions streamlines the hiring process from a single, centralized platform, resulting in a simpler, more efficient experience and faster turnaround so you and your team can spend more time on other high-value tasks.

Technology Is Our Foundation

Sterling Talent Solutions is committed to delivering the highest quality background checks combined with the fastest service in the industry. To do this, we invest in cutting-edge technologies and are constantly innovating new practices and processes at every opportunity.

Unmatched Resources

When you combine our industry-leading technologies with the deep expertise of our extensive staff of global researchers and screeners, you get an unmatchable resource for background screening excellence.

Quality of Service

Your dedicated Client Service team is there when you need them to ensure the simplest, most-effective experience for you, your team and your candidates.

Continuous Innovation

To remain highly responsive to our evolving client needs, we're continuously investing in technology and innovation. We'll keep you informed of the latest enhancements to our platform, products and integrations.

Single Hiring Solution

Get the most comprehensive background check, Form I-9 and new hire dynamic form capabilities in a single, easy-to-use platform.

Sterling
Talent Solutions

About Us

Sterling is the leader in global background screening, empowering clients to hire fast with confidence. We see the big picture, with a vision to make the world a safer place. Advanced technology, accuracy, and industry-leading turnaround time is not something that we strive for — it's our norm. That's because we hold ourselves to a higher standard. We are committed to innovation and we have the financial strength and industry expertise to make it happen.

Visit www.sterlingtalentsolutions.com

About Compliance Risk Concepts (CRC)

Compliance Risk Concepts ("CRC") is a business-focused team of senior compliance consultants and executives providing clients with critical skills and expertise required to establish, maintain, and enhance a balanced and effective compliance operation risk management program. With headquarters in New York, NY and offices in New York, NY, Chicago, IL, Houston, TX and Irvine, CA, CRC is your full-service Compliance Risk Management support partner.

To learn more, visit compliance-risk.com or contact Mitch Avnet at **mavnet@compliance-risk.com** or **(646) 346-2468**.