Advantage RISK & REGULATION

RISK & REGULATION UPDATE FROM NAVIGANT

CONTACTS »

Ellen Zimiles
Managing Director,
Head of Global Investigations
& Compliance
212.554.2602
ellen.zimiles@navigant.com

Alma Angotti
Managing Director
202.481.8398
alma.angotti@navigant.com

The Spring 2015 issue of ***Advantage: Risk & Regulation*** examines perspectives on recent global regulations that impact financial institutions and provides approaches to maximize the effectiveness of their compliance programs.

The foundation of Anti-Money Laundering (AML) compliance has always been the risk-based approach, with financial institutions having the ability to allocate resources to combat AML in a manner that is best suited for them. Regulators now have a new focus on the Customer Due Diligence rule, considering it the "fifth pillar" of AML compliance. In the leading article, ***Customer Due Diligence: The Fifth Pillar of Anti-Money Laundering Compliance***, we discuss the elements of this recent regulatory requirement and explain the actions that financial institutions will need to take to adhere to this rule.

In our ***FinCEN Human Trafficking Red Flags Advisory*** article, we provide insight on FinCEN's newly published "Guidance on Recognizing Activity that May Be Associated with Human Smuggling and Human Trafficking – Financial Red Flags" and describe the characteristics of Human Smuggling and Human Trafficking and the red flags that financial institutions should be identifying.

The Securities Exchange Commission (SEC) has observed widespread issues and deficiencies in monitoring microcap securities. Recently, the SEC announced an enforcement action against E*TRADE for failing to comply with regulatory responsibilities related to monitoring microcap securities, and simultaneously released a National Exam Program Risk Alert. Our article titled ***SEC National Program Risk Alert for Microcap Securities*** provides and overview of the SEC's alert and how broker-dealers should be reevaluating their microcap securities monitoring systems.

We hope you enjoy this issue of ***Advantage: Risk & Regulation***, the quarterly newsletter developed by the professionals in Navigant's Global Investigations & Compliance (GIC) practice to bring you insightful information and perspectives on timely and relevant industry issues that can impact your business. To read other GIC thought leadership, please visit us at **www.navigant.com/GIC**.

Please contact us if you would like to begin a dialogue on the topics covered in the newsletter or other risk and compliance issues.

Best regards,

Ellen Zimiles
Managing Director, Head of Global Investigations & Compliance

Alma Angotti
Managing Director

NAVIGANT

navigant.com/GIC

Advantage

RISK & REGULATION UPDATE FROM NAVIGANT

Customer Due Diligence: The Fifth Pillar of Anti-money Laundering Compliance

CONTACTS »

Alma Angotti
Managing Director
202.481.8398
alma.angotti@navigant.com

Christopher Daubert
Consultant
646.227.4362
christopher.daubert@navigant.com

I. INTRODUCTION

The foundation of Anti-Money Laundering ("AML") compliance has been the risk-based approach. Financial institutions have the flexibility to devote scarce resources to combat money-laundering in a manner that is best suited for their unique circumstances. However, there has been frequent criticism over the years in the lack of explicitly stated requirements that lead financial institutions towards non-compliance. The customer due diligence ("CDD") rule represents a change in the evolution of AML programs. Regulators now have a new focus towards this additional pillar within the AML program.

What this Means to You

» CDD now constitutes the new "fifth pillar" of AML Compliance.

» Identification of beneficial owners is now explicitly required for all institutions with Customer Identification Programs ("CIP").

» Financial Crime Enforcement Network ("FinCEN") regulated institutions that are not required to have CIP might soon be required to have CIP.

» There is a renewed emphasis to clearly document and justify risk-based decisions for how often to update customer information, including beneficial ownership.

» Firms should focus on their due diligence of the omnibus accountholder and establish a baseline for anticipated activity. Firms may also need to reach out to the omnibus accountholder to obtain more information to properly analyze potentially suspicious transactions. Obtaining additional information about the underlying accountholders may not be practicable if the account is located in a secrecy haven. Policies and procedures should be clear as to how to proceed (including SAR filing and account closure) if the accountholder is unable or unwilling to provide requested additional information. Firms may also need to evaluate if these types of client relationships fit into their overall risk appetite.

II. THE HISTORY LEADING TO THE CDD NOTICE OF PROPOSED RULEMAKING

In February 2012, the Financial Action Task Force ("FATF") developed its annual recommendations related to AML and Counter-Terrorism Financing ("CTF") policies. Specifically included within its recommendations about preventative measures was a regulatory requirement for CDD. "The principle that financial institutions should conduct CDD should be set out by regulation or statute. How individual jurisdictions impose specific CDD obligations may be determined through law or enforceable means."[1] A month later in March 2012, FinCEN released the Advance Notice of Proposed Rulemaking for CDD. A dialogue that consisted of both comments from financial institutions as well as a series of meetings between the regulators and financial institutions led to feedback that FinCEN incorporated into the Notice of Proposed Rulemaking.

III. THE CDD NOTICE OF PROPOSED RULEMAKING: OVERVIEW

The Notice of Proposed Rulemaking FinCEN is proposing comprises four individual regulatory requirements that act as minimum standards and collectively constitute the CDD rule. These requirements include identifying and verifying the identity of customers, identifying and verifying the identity of beneficial owners of legal entity customers (i.e., the natural persons who own or control legal entities), understanding the nature and purpose of customer relationships, and conducting ongoing monitoring to maintain and update customer information and to identify and report suspicious transactions. Additionally, there is a proposed amendment to codify this CDD rule as an additional "pillar" to AML programs as well as a timeline for implementation. A request for comments was also included with the deadline of October 3, 2014. Notably, FinCEN states in the rule-making that three out of the four regulatory requirements in the proposal are current regulatory expectations. Only the specific requirement dealing with beneficial ownership is "new."

IV. ELEMENTS OF THE CDD REQUIREMENT

A. Identifying and verifying the identity of customers.

   FinCEN recognizes that this requirement already explicitly exists as the CIP, and does not propose any changes to those provisions. The proposed rule restates this requirement as part of the CDD rule for the sake of organization and clarity.

B. Identifying and verifying the identity of beneficial owners of legal entity customers (i.e., the natural persons who own or control legal entities).

   1. Beneficial Ownership

      This is the "new" section of the proposal. Previously, the requirement to obtain beneficial ownership was "risk-based" almost in its entirety. Beneficial ownership has been addressed within specific areas of regulation. For example, Section 312 of the USA PATRIOT Act requires beneficial owners to be identified for payable-through-accounts.[2] Additionally, FinCEN guidance for money laundering risks related to shell banks clearly states the risks of Nominee Incorporation Services and the importance of identifying beneficial owners.[3] In the proposed rule, FinCEN provides explicit beneficial ownership requirements across the board by breaking down definitions, expectations, and responsibilities.

      The beneficial ownership requirement in the rule focuses on two elements: who owns the account at who controls the account.

---

1. International Standards On Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations [2012]. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.
2. Section 312 of the USA PATRIOT Act. http://www.fincen.gov/statutes_regs/frn/pdf/31_CFR_Part_103_312_EDD_Rule.pdf.
3. Potential Money Laundering Risks Related to Shell Companies (FIN-2006-G014), FinCEN. http://www.fincen.gov/statutes_regs/guidance/pdf/AdvisoryOnShells_FINAL.pdf.

a. Ownership Prong - Each individual, if any, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns 25 percent or more of the equity interests of a legal entity customer.

b. Control Prong - An individual with significant responsibility to control, manage, or direct a legal entity customer, including:

   i. An executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or

   ii. Any other individual who regularly performs similar functions.

Under the first prong, there can be no more than four (4) beneficial owners and it is possible for there to be none.[4] Regardless of how complex the legal structure exists at a given entity, beneficial ownership under this prong must be determined. Under the second prong, only 1 beneficial owner must be identified. Each prong functions independently, so it is only necessary for one condition to be met in order for beneficial ownership to exist. For example, if a controls person of an entity was an 80% owner, then the financial institution would only need to identify one person for that customer.

A contentious issue that was raised in the previous advanced notice was the approach for verification of beneficial ownership. Financial institutions were wary of the costs that would be required to determine beneficial ownership in what can often be byzantine legal structures, especially under the ownership prong. Additionally, there was concern that financial institutions would be forced to devote resources towards relatively low-risk areas at the expense of high-risk areas within the AML program.

FinCEN has determined that verification requirements extend only to the identity of a beneficial owner, not to the status of the beneficial owner. In other words, financial institutions would have to verify that the stated beneficial owner matches the driver's license provided, but would not have to undergo extensive due diligence by studying corporate records to verify that the stated beneficial owner is actually the beneficial owner.

As a result, much of the onus of determining beneficial ownership is on the customer and the information the customer provides. A concern highlighted was a potential "race to the bottom" between financial institutions in terms of what would be requested on a form provided to the customer. FinCEN created a standardized form to be used to address this concern.

2. Legal Entity Customers, Equity Interests, and Trusts

   a. Legal Entity Customer

   "Legal Entity Customer" is defined to include corporations, limited liability companies, partnerships, or other similar business entities (whether formed under the laws of a state or the United States or a foreign jurisdiction), that open a new account after the implementing date of the regulation. This would not include trusts that are not statutory business trusts.

   There are several exemptions that exist for Legal Entity Customers:

4. 10 owners each have a 10% share of an LLC. None meet the threshold within the ownership prong. 4 owners each have a 25% share of an LLC. Each owner meets the threshold within the ownership prong.

i. An issuer of a class of securities registered under Section 12 of the Securities Exchange Act of 1934 or that is required to file reports under Section 15(d) of that Act;

ii. Any majority-owned domestic subsidiary of any entity whose securities are listed on a U.S. stock exchange;

iii. An investment company, as defined in Section 3 of the Investment Company Act of 1940, that is registered with the SEC under that Act;

iv. An investment adviser, as defined in Section 202(a)(11) of the Investment Advisers Act of 1940, that is registered with the SEC under that Act;

v. An exchange or clearing agency, as defined in Section 3 of the Securities Exchange Act of 1934, that is registered under Section 6 or 17A of that Act;

vi. Any other entity registered with the Securities and Exchange Commission under the Securities and Exchange Act of 1934.

vii. A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant, each as defined in section 1a of the Commodity Exchange Act, that is registered with the CFTC;

viii. A public accounting firm registered under section 102 of the Sarbanes-Oxley Act; and

ix. A charity or nonprofit entity that is described in Sections 501(c), 527, or 4947(a)(1) of the Internal Revenue Code of 1986, that has not been denied tax exempt status, and that is required to and has filed the most recently required annual information return with the Internal Revenue Service.

b. Equity Interests

"Equity Interests" is defined as an ownership interest in a business entity. This reflects FinCEN's efforts to define the term broadly while ensuring that it can be easily understood.

c. Trusts

Trusts present an interesting challenge. While there are exceptions (statutory trusts), trusts do not fall within the scope of legal entity customer. FinCEN makes a special note that they do not consider trusts to be low-risk and that normal CIP requirements exist for the trustee. Financial institutions will have to carefully analyze the risk of their trust customers and apply the appropriate due diligence.

FinCEN seems to have adopted several practical limitations to the requirement to identify beneficial owners. The propose rule exempts intermediated account relationships and pooled investment vehicles from beneficial owner requirements. This means that only the holder of an omnibus account would be required to identify the beneficial owners of the sub-accounts, or that the clearing agent would be required to identify the beneficial owners within the pooled investment vehicle. Regulatory expectations today expect the financial institution to reach out to the intermediary for more information about the underlying account holder under certain circumstances, for example, a transaction monitoring alert or other potentially suspicious activity.

Additionally, FinCEN is considering allowing hedge funds to only identify the beneficial

owners under the "control prong" as opposed to the "ownership prong" due to how quickly the ownership structure can change.

Lastly, the provisions would apply to for all new customers; a look back would not be necessary. FinCEN, however, does recommend that all CDD information, including beneficial ownership, be as current as possible and periodically updated on a risk-based basis. The financial institution would have to consider whether to do at least a partial look back based on customer risk.

C. Understanding the nature and purpose of customer relationships.

FinCEN carefully explains the logic to support the idea that this is a precondition of existing requirements, and not a substantively new requirement. Because it is necessary to gain an understanding of all of a financial institution's customers to properly assess risk, understanding the nature and purpose of customer relationships is a component of a financial institution's responsibility to report suspicious activity. In fact, demonstrating that "no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage" is a type of suspicious activity specifically listed on the SAR form.

FinCEN acknowledges that basic account information along with typical customer information such as annual income, net worth, domicile, or principal occupation or business can build the type of customer profile that can be used as a baseline to measure what would be considered "normal business activity". There is a caveat, however, that securities and futures firms often maintain accounts for customers whose activity is based on market conditions that may have a large degree of variance in terms of activity.

D. Conducting ongoing monitoring to maintain and update customer information and to identify and report suspicious transactions.

Similar to the previously mentioned requirement about understanding the nature and purpose of customer relationships, FinCEN regards ongoing monitoring as a necessary precondition of existing responsibilities. Without this component, CDD becomes merely an exercise in collecting information. Ongoing monitoring is not just the glue that holds the other CDD components together; it is also what provides force and impact to the other CDD requirements.

Under this Notice of Proposed Rulemaking, only financial institutions that are currently covered by CIP are required to follow these requirements. This includes banks, brokers or dealers in securities, mutual funds, futures commission merchants, and introducing brokers in commodities.

E. Amendments to AML Program Requirements and Timeline to CDD Implementation

Beyond the creation of explicit CDD standards, FinCEN is proposing that the collective requirements be classified as an additional fundamental AML program requirement. This meant to stress the importance and criticality of incorporating these components into financial institution policies & procedures across the board.

CDD would become the "fifth pillar" of the AML program for all institutions covered within the scope. A slight difference exists for brokers or dealers in securities, as FINRA includes a specific program requirement for reporting suspicious activity. Though this would not necessarily change anything with regards to the FINRA program requirement, FinCEN has indicated that it will work with the SEC and FINRA to try and harmonize the requirements between regulatory bodies. The proposed Implementation deadline for all CDD requirements would be one year from when the final rule is issued.

F. Request for Comments

FinCEN identified a number of areas for further discussion with the private sector and law enforcement. In addition to seeking general comments and feedback for each topic area within the proposed CDD requirements, FinCEN seeks input about specific aspects of the CDD program.

1. Definition of Beneficial Owner
    a. Is the definition sufficiently clear?
    b. Is the term "equity interests" sufficiently clear, especially for front-line employees at financial institutions?
2. Definition of Legal Entity Customer
    a. Is the definition sufficiently clear?
3. Existing Accounts
    a. Should the proposed requirement for identifying beneficial ownership be explicitly extended to apply retroactively for existing customers?
4. Proposed Exemptions from the Beneficial Ownership Rule
    a. Intermediated Accounts
        i. Is the proposed treatment of intermediated accounts sufficiently clear?
    b. Pooled Investment Vehicles
        i. How should pooled investment vehicles that are not exempt but are operated or advised by financial institutions be treated?
    c. Trusts
        i. What procedures do financial institutions use to collect information on trusts in their CDD process?
        ii. Is information on trusts easily accessible to law enforcement?
5. Certification Form
    a. Should financial institutions be permitted to obtain the same information that the form requires through an automated electronic account opening process?
6. Verification of Beneficial Owners
    a. Is the requirement to follow existing CIP procedures for verification of beneficial owners sufficiently clear?
7. Updating of Beneficial Ownership Information
    a. Is setting a mandated timeframe for updating beneficial ownership information preferable to the proposed risk-based approach?
8. Recordkeeping Requirements
    a. Is the requirement to keep beneficial ownership recordkeeping procedures identical to CIP recordkeeping procedures sufficiently clear and efficient?
9. Understanding the Nature and Purpose of Customer Relationships and Ongoing Monitoring
    a. Are the proposed requirements sufficiently clear?
    b. Should FinCEN define the term "customer risk profile"?
    c. Can financial institutions meet SAR requirements without understanding the nature and purpose of customer relationships?
10. Proposed Amendments to the AML Program Rules
    a. Should the language for each AML program pillar be identical across all FinCEN rules?
11. Effective Date of the Rule
    a. Is one year from the date of issuance of the final rule sufficient time for implementation?

V. CONCLUSION

As Navigant stated in our client alert for the Advance Notice of Proposed Rule-Making, FinCEN is not so much making new rules as explicitly stating rules that they already expect financial institutions to be following. FinCEN seems to be balancing their desire to have AML programs function on a risk-based basis with their own frustration that certain practices have not been followed across the board.

So while the beneficial ownership rule is certainly new, its significance is probably overrated. The addition of a new "fifth pillar" of AML Program requirements is the truly radical change. Explicitly stating requirements which were once only expectations or pre-conditions for other requirements will give regulators greater power to take further action where there may have once been hesitance due to ambiguity with the requirements. However, the repackaging of these requirements into the "fifth pillar" is what demonstrates the focus of the regulators on a holistic basis. The sum becomes greater than its parts.

© 2015 Navigant Consulting, Inc. All rights reserved. 00004161
Navigant Consulting is not a certified public accounting firm and does not provide audit, attest, or public accounting services. See navigant.com/licensing for a complete listing of private investigator licenses. The opinions expressed in this article are those of the author and do not necessarily represent the views of Navigant Consulting, Inc. Neither Navigant nor the author assume responsibility for legal advice nor make any representations concerning interpretations of either the law or contracts.

Advantage

RISK & REGULATION UPDATE FROM NAVIGANT

FinCEN Human Trafficking Red Flags Advisory

CONTACT »

Balki Aydin
Senior Consultant
646.227.4658
balki.aydin@navigant.com

I. INTRODUCTION

On September 11, 2014, the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN") published the Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking-Financial Red Flags (the "Advisory"). The Advisory describes human smuggling and human trafficking and highlights the transactional and customer red flags for financial activity that may indicate human smuggling and/or human trafficking. The objective of the Advisory is to assist financial institutions in detecting and investigating these red flags and reporting to law enforcement agencies as appropriate.

II. WHAT IS HUMAN SMUGGLING/TRAFFICKING?

A. Human Smuggling:

Per the Advisory, the term "human smuggling" is an act or attempt to bring foreign nationals illegally to the U.S. through air, sea or land travel and transport them within the U.S. Illegal migrants usually seek for help from local smugglers in other countries, mostly in Mexico and countries in Central America to cross the border to the U.S. Payments are either made full in advance, on arrival or in installments depending on the situation.

B. Human Trafficking

The Advisory describes "human trafficking" as the act of coercing and exploiting victims against their will for forced labor, commercial sex work and involuntary participation in crimes. Human trafficking victims can be anyone regardless of their nationality, age or sex and geographical location through deception such as false marriages, fake employment and study abroad opportunities and through force such as kidnapping. After being collected through recruitment or abduction, victims may be transported domestically or internationally by air, sea and /or land to be exploited or sold to other traffickers. Human trafficking may generate ongoing criminal proceeds whereas human smuggling is a one-time illicit activity.

What this Means to You

- Provide training to your employees regarding the red flags of human trafficking and human smuggling
- Include human trafficking and human smuggling indicators in your compliance programs
- Train bank tellers to detect suspicious behaviors of the customers that might be related to human trafficking and human smuggling
- Build transaction monitoring systems to identify financial account activity with the indicators of human trafficking and human smuggling

III. GUIDANCE TO FINANCIAL INSTITUTIONS

A. Overall, financial institutions can detect and evaluate suspicious activity through:

1. Reviewing transactions at the relationship level rather than at the account level;
2. Advising branch or floor personnel to observe customer behavior through direct interaction to detect suspicious or unusual behavior and conduct a review of the customer's transactions if necessary;
3. Sharing information voluntarily with other financial institutions as appropriate under section 341(b) of the USA Patriot Act[1] regarding suspected money laundering activity involving human smuggling/ trafficking;
4. Filing a SAR on suspicious transactions that are possibly related to human smuggling/ trafficking by using the key terms "Advisory Human Smuggling" and/or "Advisory Human Trafficking" with supporting information for the financial transaction activity.

B. Common Red Flags of Human Smuggling and Human Trafficking

1. Transfers or deposits below $3,000 to avoid the record keeping requirement or below or equal to $10,000 to evade Currency Transaction Reports (CTRs);
2. Potential funnel accounts belonging to individuals or businesses that receive cash deposits below or equal to the $10,000 reporting threshold which are withdrawn in different geographical locations shortly after deposits are made;
3. Frequent cash deposits and wire transfers in high dollar amounts that are inconsistent with the expected account activity;
4. Different originators using similar transaction information such as the same phone number, address and transactions in similar amounts. These originators usually have no evident relationship to each other and to the beneficiary and cannot provide sufficient information about the purpose of the funds;
5. Transactional activity and/or lifestyle is incompatible with business line or employment;

C. Red Flags Specific to Human Smuggling

1. Multiple wire transactions sent from various locations, especially countries with high migrant populations such as Mexico, Honduras, Guatemala and El Salvador to a U.S. or Mexican city along the Southwest Border (U.S.-Mexico land border).
2. Wire transfers originated along the Southwest Border on the same day or on consecutive days at different branches of the same financial institution;

1. Pub. L. No. 107-56, § 314(b). See also, 31 CFR 1010.54.

3. New customers acting on behalf of customers whose accounts near the Southwest border were closed due to suspicious activity and who are conducting similar repetitive cash intensive account activity to those closed accounts.

D. Red Flags Specific to Human Trafficking

1. Business accounts that have very little or non-existent payroll expenditures (e.g. wages or social security contributions) that are inconsistent with their business size and activity;
2. Business accounts with apparent deductions in employee wages under various cost types such as housing and food;
3. Cashed payroll checks where the majority of the funds are either deposited back into the employer's account or kept by the employer;
4. Customer visits to the branch with third party escorts who may act as an interpreter and may keep the customer's ID in their possession;
5. Recurring transactions conducted in a business account for various expenditures such as the payment of housing, vehicle rentals and/or living expenses that are inconsistent with the business line;
6. Accounts of various foreign workers or students where a common employer/employment agency serve as a custodian.

IV. CONCLUSION

In summary, no one transaction or account activity is a solid definitive indicator of human smuggling and/or human trafficking. Financial institutions should consider the red flags of human trafficking and human smuggling described in the guidance along with other factors such as the customer's profile or business type and expected account activity. If the institution has "reason to suspect" that the activity is related to human smuggling or human trafficking, it should report the activity by filing a SAR.

© 2015 Navigant Consulting, Inc. All rights reserved. 00004161
Navigant Consulting is not a certified public accounting firm and does not provide audit, attest, or public accounting services. See navigant.com/licensing for a complete listing of private investigator licenses.
The opinions expressed in this article are those of the author and do not necessarily represent the views of Navigant Consulting, Inc. Neither Navigant nor the author assume responsibility for legal advice nor make any representations concerning interpretations of either the law or contracts.

Advantage

RISK & REGULATION UPDATE FROM NAVIGANT

SEC National Program Risk Alert for Microcap Securities

CONTACTS »

Alma Angotti
Managing Director
202.481.8398
alma.angotti@navigant.com

Brian Chan
Senior Consultant
646.227.4297
brian.chan@navigant.com

Christopher Daubert
Consultant
646.227.4362
christopher.daubert@navigant.com

I. INTRODUCTION

On October 9, 2014, the Securities and Exchange Commission ("SEC") announced an enforcement action against E*TRADE for failing to comply with regulatory responsibilities related to monitoring unregistered sales of microcap stocks on behalf of their customers. E*TRADE sold billions of penny stock shares for customers without fulfilling its obligation to conduct reasonable inquiry under Securities Act Section 4(a)(4). Though no Anti-Money Laundering ("AML") charge was included in the Enforcement Action, E*TRADE was cited for an AML deficiency related to how it performed due diligence. E*TRADE settled with the SEC by agreeing to pay back $1.5 million in disgorgement and prejudgment interest from commissions earned from improper sales, as well as an additional $1 million fine.[1]

The SEC also simultaneously released a National Exam Program Risk Alert to inform broker-dealers of their industry-wide findings related to sales of microcap stocks.

What this Means to You

- The SEC has observed widespread issues related to the monitoring of microcap stocks and has put broker-dealers at large on notice.
- Broker-dealers should reevaluate their risk assessment for sufficient criticality and depth.
- Broker-dealers should reevaluate any operations and compliance monitoring systems in place.
- Broker-dealers should reevaluate detection scenarios in place to generate alerts related to deliveries of microcap stocks and market manipulation.
- Broker-dealers should reevaluate policies and procedures in place to monitor and investigate indications of illicit transactions of microcap securities.

1. Order Instituting Administrative and Cease-and-Desist Proceedings in the Matter of E*Trade Securities, LLC, and G1 Execution Services, LLC. http://www.sec.gov/litigation/admin/2014/33-9662.pdf

II. NATIONAL EXAM PROGRAM RISK ALERT

A. Overview

The SEC Risk Alert makes it clear that deficiencies in monitoring microcap securities are widespread. Specifically, the SEC noted that the Office of Compliance Inspections and Examination ("OCIE") had inspected 22 broker-dealers in microcap security sales and more than 80% were issued letters of deficiency for material control weaknesses and/or potential violations of law.[2] While most of the broker-dealers had policies and procedures on the books, there was generally either a lack of sufficient detail in the procedures or inherent weaknesses in internal controls. As a result, the broker-dealers either 1) failed to conduct reasonable inquiry as required under Securities Act Section 4(a)(4); 2) failed to respond adequately to suspicious activity as required under the Bank Secrecy Act ("BSA") or 3) failed to provide additional inquiry on accounts particularly susceptible to unregistered sales of securities.

B. Failure to Conduct Reasonable Inquiry under Securities Act Section 4(a)(4)

Under Securities Act Section 4(a)(4), broker-dealers have a responsibility to conduct a "reasonable inquiry" to determine if a customer's transaction is not exempt from Section 5 of the Securities Act. This means that the firm must conduct due diligence to determine if a customer's securities either have a proper registration statement or exemption from the Section 5 requirement. The risk alert noted some observations from SEC Staff:

1. Some firms' policies and procedures did not contain sufficient detail to guide employees in efforts to monitor for and identify violations;
2. Some firms relied solely on the absence of restrictive legends on stock certificates as sufficient evidence that the securities could be resold in unregistered transactions;
3. Some firms relied solely on the fact that the delivery of the shares into a customer's account came from the Depository Trust and Clearing Corporation ("DTCC") as a basis for believing that the shares were not restricted securities; and
4. Some firms did not collect information from the customer when large blocks of shares were delivered in with a subsequent order to sell.

One key inference is that there is no substitute for performing proper due diligence on the delivery of securities. Additionally, the mere existence of policies and procedures is not enough; the policies and procedures should be detailed, supplemented with proper controls, and effective.

C. Failure to Respond to Suspicious Activity

The SEC did not charge E*TRADE with having a deficient AML compliance program or with failing to file Suspicious Activity Reports (SARs). The SEC pointed out in the risk alert its finding that other broker-dealers failed to follow the Section 5 and AML policies and procedures that actually were in place. Broker-dealers were aware of several key indications of market manipulation or the distribution of unregistered securities, yet they failed to file SARs as required under the BSA when:

1. There was atypical trading patterns in the issuers' securities, including trading involving sudden spikes in price and volume;

2. SEC National Exam Program Risk Alert: Broker-Dealer Controls Regarding Customer Sales of Microcap Securities. http://www.sec.gov/about/offices/ocie/broker-dealer-controls-microcap-securities.pdf

2. Certain patterns of trading activity being common to several customers, including, but not limited to the sales of large quantities of the shares of multiple issuers by the customers;
3. Notifications received from the broker-dealers' clearing firms that the clearing firms had identified potentially suspicious activity in the securities of certain issuers or certain of the broker-dealers' customer accounts. Such notifications took the form of alerts, expressions of concern, or actions taken by the clearing firms to restrict trading in certain issuers' securities and/or certain customer accounts;
4. The involvement of certain types of accounts, including those that provide anonymity to the beneficial owners in the liquidation of the shares of the microcap issuers; and
5. Requests received from FINRA for information relating to certain issuers and the broker-dealers' customer accounts.

D. Additionally, the SEC noted that other indications of suspicious activity were readily discoverable by the broker-dealer staff, including certain types of issuer information such as:

1. Nominal assets and low operating revenue,
2. Frequent changes to the type of activity in which the business was engaged, the name of the corporate entity, directors, and/or management; and
3. Sales through the broker-dealer by individuals known throughout the industry to be stock promoters.

The SEC has essentially found fault with broker-dealers for not acting on information they had and alternatively, not taking action to learn more in specific scenarios to investigate red flags and filing SARs as appropriate.

E. Types of Accounts Used to Dump Microcap Stock

In what has been a recurring theme this year, the SEC noted that omnibus accounts were particularly useful in facilitating illicit transactions with large blocks of microcap stock. Examples of omnibus accounts included:

1. Accounts of purported stock loan companies, which may hold the restricted securities of corporate insiders who have pledged the securities as collateral for, and then defaulted on, purported loans, after which the securities are sold on an unregistered basis;
2. Accounts held in the name of a corporate entity (or LLC), either for the company's own use or as a third-party custodian on behalf of other beneficial shareholders or customers, which disguise the unregistered sales of securities owned by corporate insiders of the company and allow for those insiders to withdraw proceeds individually;
3. Accounts held in the names of foreign financial institutions, such as offshore banks and/or broker-dealers that sold shares of the stock on an unregistered basis on behalf of customers, who may have been stock promoters; and
4. Accounts using a master/sub-structure, which allows for trading anonymity with respect to the sub-accounts' activity.

Transparency is one of the key variables in evaluating AML risk for products, accounts, and services. The SEC is reinforcing the basic premise that accounts with less transparency, such as omnibus accounts, carry higher risk and should be monitored accordingly.

III. CONCLUSION

The common issues that the SEC illustrates in the Risk Alert should give pause to those who assume that status-quo compliance programs are sufficient in dealing with the challenges related to microcap securities. There are several questions Compliance Officers at broker-dealers should be asking themselves:

A. Have we properly assessed the risk of our clients, accounts, products, and services?

   This should be the starting point for every compliance program, and too often problems result due to a lack of criticality or depth in the evaluation of the business.

B. Do we have a sufficient monitoring system in place?

   There is often significant pressure to "make do" with outdated operations and compliance systems for several reasons, such as cost pressures and mere inertia. Upholding regulatory requirements with the proper tools can be challenging, but upholding regulatory requirements without the proper tools is almost impossible.

C. Have we developed and tuned detection scenarios that can generate quality alerts for investigation?

   Not having the right detection scenarios is a sure route towards non-compliance, but improper tuning of detection scenarios also leads to the same path. Cost pressures can cause institutions to try and skimp on tuning, leading to default "out of the box" scenarios. The problem is that every financial institution is different, and no "out of the box" scenario can account for the unique circumstances at each firm. If a detection scenario creates too many false positives, analysts become conditioned to close alerts with minimal investigation.

D. Do we have detailed and thorough policies and procedures?

   Having the right tools is only one part of the equation; having analysts who understand how to properly use the tools is the other part of the equation. The SEC noted that many broker-dealers were aware of key indications of improper sales of securities, but the policies and procedures in place did not assist employees in investigations.

E. Do we have appropriate procedures to escalate potentially suspicious trading activity for analysis and SAR reporting?

   Often, there is a lack of training of and/or communication between trading surveillance staff and the BSA staff. At a minimum, the firm should train trading surveillance staff to identify and escalate potentially suspicious patterns of trading activity for analysis and SAR reporting as appropriate.

By issuing the Risk Alert, the SEC has made it clear that ignorance is no longer an excuse for non-compliance when it comes to monitoring unregistered securities.

© 2015 Navigant Consulting, Inc. All rights reserved. 00004161
Navigant Consulting is not a certified public accounting firm and does not provide audit, attest, or public accounting services. See navigant.com/licensing for a complete listing of private investigator licenses.
The opinions expressed in this article are those of the author and do not necessarily represent the views of Navigant Consulting, Inc. Neither Navigant nor the author assume responsibility for legal advice nor make any representations concerning interpretations of either the law or contracts.