CORE COMPLIANCE & LEGAL SERVICES, INC.
SOLUTIONS FOR TODAY'S BUSINESS

Risk Management Update
May 2013

REGULATORY UPDATE: NEW IDENTITY THEFT RULE

In 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") amended the Fair Credit Reporting Act ("FCRA") section 615(e) to include the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC") to the list of federal agencies that must jointly adopt and separately enforce regulation of identity theft red flags. To that end, on April 10, 2013, the SEC and the CFTC jointly issued their final rules and guidelines for entities regulated by each of the respective agencies under Regulation S-ID – Identify Theft Red Flags Rules (the "Rule" or "Regulation S-ID").[1] The new regulation became effective on May 20, 2013 and requires all affected firms to have policies and procedures in place by November 20, 2013.

Background

Advancements in electronic communication and technology increase the ease to capture a client's personal information, which too, increases potential threat to safeguard confidential and private information. To address these concerns, stronger rules and regulations geared toward protecting consumer private personal information are enacted. Regulation S-ID is very similar to previously issued regulations by the Federal Trade Commission ("FTC") under the Bank Secrecy Act ("BSA"), which applies to "financial institutions" (as defined below) and "creditors."[2] The new Rule provides additional guidance and transfers enforcement from the FTC to the SEC and CFTC as required under the Dodd Frank Act. Regulation S-ID expands the definition of financial institutions and may extend to entities regulated by the SEC and CTFC that previously had not been required to implement identity theft programs under the BSA.

For purposes of this Rule, a "financial institution" is an SEC regulated entity that is:

- A broker-dealer or any person that is registered or required to be registered under the Exchange Act of 1934 ("Exchange Act");
- An investment company that is registered or required to be registered under the Investment Company Act of 1940 (the "'40 Act") , that has elected to be regulated as a business development company under the '40 Act, or that operates as an employees' securities company under the '40 Act; or
- An investment adviser that is registered or required to be registered under the Investment Advisers Act of 1940 ("Advisers Act")[3]

---

[1] *See* http://www.sec.gov/rules/final/2013/34-69359.pdf
[2] Generally includes persons extending credit, but excludes certain "incidental credit providers," such as advisers who bill in arrears.
[3] *See* Id.

The final rule requires that the above financial institutions that offer or maintain a "covered account"[4] establish a Identity Theft Prevention program to detect, prevent, and mitigate identity theft for existing and new client accounts. The rule states that the program should be customized and designed according to the size and complexity of each firm's business model and focus on identifying "red flags."

Importantly, even if a financial institution does not meet the above criteria set forth in the rule, it is important to develop this program in order to safeguard client assets, satisfy fiduciary obligations and protect accounts that may have a foreseeable risk of identity theft.

What is a Red Flag?

A red flag means a pattern, practice, or specific activity that indicates the possible existence of problem. In the case of identity theft,[5] Red Flags are typically found in the following scenarios:

1. Electronic alerts, notifications, or other warnings are received from consumer reporting agencies, service providers (such as a fraud detection service) or others signaling that an outsider is attempting to assume someone's identity;
2. At account opening, suspicious documents are received which appear to have been altered or forged;
3. Frequent requests for changes to personal contact information, such as a suspicious address change or changing to a P.O. Box;
4. After a recent change of address, the firm is asked to add another person to the account;
5. Suspicious activity, such as large outgoing wires, that occurs within a client's account or checks sent to a different address than the account holders;
6. Notification from a client or law enforcement agency that the client is or appears to be a victim of identity theft in connection with client accounts held by the firm.
7. Notification from a client that they are not receiving their account statements in the mail;
8. A person calling in to obtain account information cannot provide identifying information, such as account number, social security number, account registration and address of record.

Summary of New Rule Requirements for Identity Theft "Red Flags"

In developing policy and procedure safeguards for preventing identity theft, Regulation S-ID provides that firms should do the following:

- Identify and Detect Relevant "Red Flags" for Covered Accounts - a firm's program must be able to have internal controls to ***identify*** and ***detec***t relevant red

[4] Summarily, a covered account is an account whereby a financial institution may direct payments to a third-party from a client account (i.e., a transaction account) or pays bills on behalf of clients.
[5] Id.

flags, such as through checks by third-party administrators, internal account opening protocols and processes for identifying clients who are calling in.

- Effectively Respond to Red Flags Detected – the policies and procedures implemented by the firm should address what escalation procedures should occur if red flags are detected, including who will ***respond***, the timeliness of the response and mitigation of potential and actual risks.
- Periodically Review and Update Your Identity Theft Prevention Program – Identity theft prevention requires the program to be continuously reviewed and not stagnant. Policies and procedures should be reviewed frequently, particularly as technologies enhance or business models change which requires firms to periodically ***update*** the program to reflect changes in risks to clients and the firm from identity theft.

Designing Your Firm's Identity Theft Program

When designing your Identify Theft Program think, begin by evaluating the protocols used by your organization, and particularly during account opening and outgoing wire process. What types of accounts does the firm offer; how are accounts opened; what methods are used to access an account by clients; and has the firm or client had a previous experience involving potential or actual identify theft.

If the firm has not experienced potential or actual identity theft in the past, become familiar with the different types of identity theft that can occur as this will help in developing internal safeguards to protect against risks.

Next, consider who will oversee the program and what actions are required. For example, conduct due diligence of the firm's third-party service providers and request certifications relating to their identity theft prevention protocols. Consider existing privacy and information security policies and how the firm satisfies "KYC" (know your client) obligations. Finally, consider what internal controls could be enhanced to help safeguard against identity theft. Develop protocols to further monitor client transactions and to look for suspicious activities and potentially altered documents. Verify change of address requests through phone calls or letter notifications, sending a letter both to the old and new addresses of records.

A key component of the program must be training for all employees to effectively implement your program. It is critical for operational personnel to know and understand what to look for so they can assist with detection and prevention of potential identity theft.

Once an alert system is established, develop oversight and escalation procedures on what should occur if / when identity theft occurs. This may include:

- Notification to the client and credit reporting agency of potential fraud;
- Changing passwords, security codes, and/or other security devices that permit access to a client's account;

- Reopening a client's account with a new account number;
- Closing the existing client account or place a freeze on the account;
- Not attempting to collect on a client's account or not selling a client's account to a debt collector;
- Notifying law enforcement; and/or
- Determining that no response is warranted under the particular circumstances.

Oversight of the Identity Program by the Board of Directors ("Board") or senior management team is critical. Specific responsibilities should be assigned, which includes review of periodic and annual reports evidencing the effectiveness of the Identity Theft Prevention program. Once the firm has written an identity theft program, it must be approved by either the Board or senior management.

Pursuant to the rule, no less than on an annual basis, a report must be provided to the Board or senior management team on the firm's compliance with the program. Such reports should address material matters related to red flags detected and identified and include an evaluation of the effectiveness of the policies and procedures in identifying and addressing risks associated with identity theft.

Conclusion

While the compliance date of the Rule is not until November 2013, it is important to get started now. If your firm already has red flag rules in place, review your present policies and procedures and enhance where needed to comply with the new regulation. If you do not have a program in place, consider some of the above examples of how identity theft may occur, and evaluate the best ways utilizing existing and potentially new resources to detect and prevent identity theft before it occurs.

For more information or to learn about how Core Compliance & Legal Services, Inc. may be of assistance with your annual review process and procedures, please do not hesitate to contact us at (619) 278-0020.

Authors: Kris Gruben, Sr. Compliance Consultant and Michelle L. Jacko, CEO, Core Compliance & Legal Services ("CCLS"). CCLS works extensively with investment advisers, broker-dealers, investment companies, hedge funds, private equity firms and banks on regulatory compliance issues. For more information about this topic and other compliance consultation services, please contact us at (619) 278-0020, info@corecls.com or visit www.corecls.com.