September 2013

Regulatory brief

A publication of PwC's financial services regulatory practice

Identity Theft Regulation: Are you under the SEC/CFTC microscope?

Overview

Easy access to information has made it increasingly common for hackers and thieves to collect and share personal information about individuals. Congress initially responded to this problem by amending the Fair Credit Reporting Act ("FCRA") in 2003, mandating that certain federal agencies adopt rules requiring organizations to implement programs for detecting and preventing identity theft ("ID Red Flag Rules").[1] Although these rules applied to many entities that were also registered with the Commodity Futures Trading Commission ("CFTC") and the Securities and Exchange Commission ("SEC"), neither the SEC nor the CFTC issued its own ID Red Flag Rules at the time. Consequently, neither the SEC nor the CFTC examined their registrants for compliance or enforced the rules.

However, in April of this year, as required by the Dodd-Frank Act, the SEC and CFTC jointly adopted a rule for the prevention of identity theft, called Regulation S-ID ("Reg S-ID" or "Rule"). The Rule is similar to the ID Red Flag Rules previously enacted by the other agencies, though the SEC and CFTC provide additional guidance on its scope and application for SEC and CFTC registrants.

The Rule requires SEC or CFTC registrants (e.g., investment advisers, investment companies, broker-dealers, commodity pool advisors, futures commission merchants, retail foreign exchange dealers, commodity trading advisers, introducing brokers, swap dealers, and major swap participants) to establish and maintain programs that detect, prevent, and mitigate identity theft, if they maintain certain types of accounts for clients. These organizations must implement Reg S-ID policies and procedures by November 20, 2013.

Importantly, while they may have been covered by prior ID Red Flag Rules, SEC and CFTC registrants are now subject to oversight by the SEC and CFTC with respect to these rules. With the implementation date approaching, we are seeing that impacted organizations are beginning to finalize their approach.

This **Financial Services Regulatory Brief** clarifies which organizations will be subject to Reg S-ID, assesses the impact of the Rule's requirements, and provides our view of industry best practices for satisfying the Rule.

---

[1] The FCRA amendments required ID Red Flag Rules to be enacted by the Office of the Controller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission.

pwc

Impacted CFTC and SEC registrants

Reg S-ID applies to all financial institutions or creditors that offer or maintain a "covered account." The SEC and CFTC have created slightly different designations of which organizations are "financial institutions" or "creditors" covered by the new Rule.

SEC scope and definitions

SEC-regulated entities that are deemed a financial institution or creditor (as defined by the FCRA) are covered by Reg S-ID. The SEC stated that it expects broker-dealers, investment companies, and investment advisers to fall under these definitions.

As detailed on the next page, the SEC also stated that these entities must hold a "covered account," such as a "transaction account" belonging to an individual, in order to be subject to Reg S-ID. The SEC provided the following as illustrative examples:[2]

(i) A broker-dealer that offers custodial accounts;

(ii) A registered investment company that enables investors to make wire transfers to other parties or that offers check-writing privileges; and

(iii) An investment adviser that directly or indirectly holds transaction accounts and is permitted to direct payments or transfers out of those accounts to third parties.

Some commenters requested that the SEC exempt investment advisers from Reg S-ID under the theory that investment advisers do not generally "hold" transaction accounts. The SEC disagreed, however, stating that "[i]nvestment advisers who have the ability to direct transfers or payments from accounts belonging to individuals to third parties upon the individuals' instructions, or who act as agents on behalf of the individuals, are susceptible to the same types of risks of fraud as other financial institutions."[3]

Underscoring this point, during the SEC's open meeting to discuss the Rule, SEC Commissioners expressed concern that imposters could pose as investors and ask investment advisers to transfer money to a fraudulent third party. As a result, investment advisers are subject to Reg S-ID because "[i]nvestors who entrust their assets to registered investment advisers that directly or indirectly hold transaction accounts should receive the protections against identity theft provided" by the new regulation.[4]

In addition, SEC registrants that are considered a "creditor" are also subject to the Rule. For SEC purposes, a "creditor" is a person that "regularly and in the course of business … advances funds to or on behalf of a person" with the expectation of repayment.[5] Again, some commenters questioned whether an investment adviser would fit under this definition. The SEC responded that an investment adviser "could potentially qualify as a creditor if it 'advances funds' to an investor that are not for expenses incidental to services provided by that adviser," such as a bridge loan from an adviser to an investor prior to the adviser receiving investor money from a capital call.[6]

CFTC scope and definitions

The CFTC took a slightly different approach from the SEC when identifying financial institutions and creditors covered under Reg S-ID. As with the SEC approach, all financial institutions and creditors covered by the FCRA are considered in scope.

The CFTC identified a broad list of entities it felt were likely to "directly or indirectly" hold a covered account such as a transaction account belonging to a consumer, and thus be subject to the Rule.[7] The CFTC singled out the following entities: any futures commission merchants, retail foreign exchange dealers, commodity trading advisors, commodity pool operators, introducing brokers, swap dealers, or major swap participants.[8] The CFTC stated that these types of entities were included because they are likely to come into possession of individual personal information.

Although swap dealers and major swap participants may not interact directly (or indirectly) with consumers, these organizations have been specifically identified by the CFTC as in-scope entities and should undertake the analysis set forth below to determine whether they are covered by the Rule.

In addition, the FCRA definition of "creditor" is applied to any of the types of entities enumerated above that either: regularly extend, renew, or continue credit; arrange for such credit activities; or participate as an original creditor's assignee in the decision regarding such credit activities.[9]

---

[2] Rule, p. 16, http://www.sec.gov/rules/final/2013/34-69359.pdf.

[3] Rule, p. 17.

[4] Rule, p. 17.

[5] 15 U.S.C. 1681(m)(e)(4)(A)(iii).

[6] Rule, p. 23.

[7] 17 CFR part 162.30(b)(7).

[8] 17 CFR part 162.1(b).

[9] 17 CFR part 162.30(b)(5).

Covered accounts

Only those financial institutions and creditors that offer or maintain a "covered account" are subject to the Rule. A covered account is:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions (i.e., a transaction account); or

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputational, or litigation risks.[10]

An "account" is defined as a "continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes."[11]

Is your organization required to comply with Regulation S-ID?

The new rules require financial institutions and creditors to first determine whether they have covered accounts and, if so, to comply with Reg S-ID.

Determining Steps for Reg S-ID Compliance

Is my organization a "financial institution" registered with the SEC or CFTC?

If **no**, no further action required.

If **yes**, does the organization offer or maintain a "covered account" primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions (i.e., a transaction account)?

If **no**, periodically re-evaluate whether there are any covered accounts.

If **yes**, develop, implement, and regularly evaluate a written red flag program.

We suggest that financial institutions and creditors perform periodic assessments of covered accounts. Organizations that do not have covered accounts should periodically reassess whether a program should be implemented due to business changes, while organizations with covered accounts that have established a compliance program should periodically assess whether the organization's risk profile has changed, requiring updates or enhancements to its existing program. These assessments should consider the following:

(i) The methods an entity provides to open its accounts;

(ii) The methods an entity provides to access its accounts; and

(iii) The entity's previous experience with identity theft.

Both the SEC and CFTC addressed the possibility that only a subset of an entity's accounts present a "reasonably foreseeable risk to customers." In these instances, the Rule would only apply to those select accounts or account types.

How will Reg S-ID impact your organization?

If your organization has covered accounts, it is required to implement a written red flag program to "detect, prevent, and mitigate" the risk of identity theft ("Identity Theft Program" or "program"). The Rule provides flexibility regarding the program's elements as long as they are adequate given the organization's size and complexity.

Regulators provided the following guidance on establishing an Identity Theft Program:

Identify relevant red flags: The program should include reasonable policies and procedures to identify relevant red flags for covered accounts. Organizations should consider the following categories of red flags:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- Presentations of suspicious documents, such as documents that appear to have been altered or forged;
- Presentation of suspicious personal identifying information, such as a suspicious address change;
- Unusual use of, or other suspicious activity related to, a covered account; and
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

[10] 17 CFR part 162.30(b)(3) (CFTC) and 17 CFR part 248.201(b)(3) (SEC).

[11] 17 CFR part 162.30(b)(1) (CFTC) and 17 CFR part 248.201(b)(1) (SEC).

Detect red flags: Policies and procedures implemented for the purpose of detecting red flags should consider both new and existing covered accounts. For new accounts, organizations should verify the identity of the person opening a covered account through evidentiary documentation. For existing accounts, organizations should verify the validity of any change of address requests. Transactions should be monitored for the appearance of fraudulent activity.

Prevent and mitigate identity theft: Organizations should determine appropriate escalation procedures for red flags based on their degree of risk, including consideration of factors that heighten the possibility of identity theft. Possible responses include account monitoring, closing or refusing to open a new account, contacting the customer or law enforcement, or determining that no response is warranted. Organizations would be wise to document the escalation and resolution of red flags.

Update the Identity Theft Program: An organization's ongoing risk assessment should consider the following factors when determining whether to update its Identity Theft Program: "(i) the experiences of the financial institution or creditor with identity theft; (ii) changes in methods of identity theft; (iii) changes in methods to detect, prevent, and mitigate identity theft; (iv) changes in the types of accounts that the financial institution or creditor offers or maintains; and (v) changes in the business arrangements of the financial institution or creditors, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements."[12]

Management oversight: In addition to program requirements, the Rule requires that organizations institute oversight controls from the board of directors, a management committee, or a designated senior management employee, as applicable. These controls consist of (i) approving the Identity Theft Program, (ii) assigning specific responsibility for the program's implementation, (iii) reviewing reports prepared by staff regarding compliance by the financial institution or creditor with the final Rule, and (iv) approving material changes to the program as necessary to address changing identity theft risks.

Training: Financial institutions and creditors have an obligation to train staff, as necessary, in the effective implementation of the Identity Theft Program.

[12] Rule, p. 38.

Annual reporting: On an annual basis, it is the responsibility of staff developing, implementing, and administering the program to report any material issues, the overall program effectiveness, any significant incidents of identity theft, and recommendations for material changes to the program to the Board of Directors, management committee, or designated senior management employee.

Oversight of service provider agreements: Financial institutions and creditors that engage a service provider to perform an activity in connection with its covered accounts should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Organizations remain legally responsible for the actions taken by third party service providers.

Actions to take when implementing Reg S-ID

There is no-one-size-fits all solution when setting up an Identity Theft Program, but there are controls that should be enhanced, amended, and leveraged to comply with Reg S-ID requirements. Organizations should consider taking the following actions:

1. Amend your policies and procedures to include a periodic review of: (a) whether your organization is a financial institution or creditor; and (b) whether you offer or maintain covered accounts. This review could be incorporated into your annual compliance testing.
2. Incorporate existing policies, procedures and controls into your Identity Theft Program that are designed to quell identity theft risks. For example, current infrastructure for new client onboarding can be used for red flag detection. SEC registrants should also consider enhancing or amending the privacy controls that currently exist in connection with Reg S-P.
3. Identity Theft Programs should be customized to your organization. Withhold the temptation to include every SEC and CFTC suggestion unless they are all applicable to your operations.
4. Amend annual employee training to include specific training on implementation and management of your Identity Theft Program.

www.pwcregulatory.com

Additional information

For additional information about PwC's Financial Services Regulatory Practice and how we can help you, please contact:

Dan Ryan
Financial Services Regulatory Practice Chairman
646 471 8488
daniel.ryan@us.pwc.com

Alison Gilmore
646 471 0588
alison.gilmore@us.pwc.com

Contributors: David Harpest, Elizabeth Crotty, Matthew Shankoff, Phyllis Cela, and Lori Richards.

To learn more about financial services regulation from your iPad or iPhone, click here to download PwC's new Regulatory Navigator App from the Apple App Store.

Follow us on Twitter @PwC_US_FinSrvcs