March 7, 2012

CFTC and SEC Jointly Propose Identity Theft Rules

Contents

On February 28, 2012, the CFTC and the SEC proposed rules and guidelines requiring financial institutions and other creditors under their respective jurisdiction to develop written identity theft prevention programs.

In addition, the Commissions proposed change of address rules that would apply to any financial institution or creditor under their jurisdiction that issue credit or debit cards to consumers.

The proposed rules were required by the Dodd-Frank Act, which added the CFTC and SEC to the list of federal agencies that were required to issue rules to prevent identity theft. The Commissions' proposed rules are substantially similar to final rules and guidelines that were issued jointly in 2007 by the OCC, the Federal Reserve, the FDIC, the OTS, the National Credit Union Administration, and the FTC.[1] The Commissions noted in their joint proposing release that it is likely that most of the financial institutions and creditors covered by the proposal already comply with existing rules to prevent identity theft, and therefore may only be required to supplement programs already in place.

Identity Theft Prevention Program

Entities Required to Comply

Financial Institutions and Creditors

The proposed rules require financial institutions and certain creditors that fall under the jurisdiction of either the CFTC or the SEC, and that offer or maintain covered accounts, to implement a program to prevent identity theft. Under these proposed rules, the terms "financial institution" and "creditor" carry the same meanings as they do under the Fair Credit Reporting Act of 1970 (the "**FCRA**").[2]

The CFTC's proposed rules define the term "financial institution" to include any futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker,

[1] *See* Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 FR 63,718 (Nov. 9, 2007).

[2] Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 15 U.S.C. § 1681 *et seq.*). The term "financial institution" is defined in 15 U.S.C. 1681a(t), and the term "creditor" is defined in 15 U.S.C. 1681m(e)(4). The term "creditor" was amended by the Dodd-Frank Act for the purposes of identity theft red flag rules and guidelines, and the Commissions' proposed definition reflects this amendment.

Definition of Financial Institution

Financial institution is defined under the FCRA as:

- a State or National Bank;
- a State or Federal savings and loan association;
- a mutual savings bank;
- a State or Federal credit union; or
- any person that, directly or indirectly, holds a "transaction account" belonging to a customer.

Transaction account is defined under the Federal Reserve Act, and means a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawals, telephone transfers or other similar items for the purpose of making payments or transfers to third persons or others. The term includes:

- demand deposits;
- negotiable order of withdrawal accounts;
- savings deposits subject to automatic transfers; and
- share draft accounts.

swap dealer or major swap participant that directly or indirectly holds a transaction account for a customer.

The CFTC states that the term "creditor" will include the same entities listed above if they:

- regularly extend, renew or continue credit;
- regularly arrange for the extension, renewal or continuation of credit; or
- in acting as an assignee of an original creditor, participate in the decision to extend, renew or continue credit.

The SEC's proposed rules define the terms "financial institution" and "creditor" only by reference to the FCRA. However, the SEC states that registered broker-dealers, investment companies, and investment advisors fall within the scope of the rule. The SEC does not anticipate that the scope of the rule will cover nationally recognized statistical rating organizations, self-regulatory organizations, municipal advisors or municipal securities dealers.

Furthermore, under the SEC's proposed rules, the term "creditor" will include:

- lenders such as brokers or dealers offering credit accounts;
- securities lending services; and
- short selling services.

Entities that Offer Covered Accounts

Financial institutions and creditors are only required to comply with the proposed rules if they offer or maintain "covered accounts." Covered accounts include:

- accounts offered or maintained primarily for personal, family or household purposes, that involve or are designed to permit multiple payments or transactions; and
- any other account where there is a foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

For financial institutions and creditors subject to the CFTC's jurisdiction, covered accounts will include margin accounts, and for those entities subject to SEC oversight, covered accounts include brokerage accounts and accounts maintained by a mutual fund that permit wire transfers or other payments to third parties.

The proposed rules require that financial institutions and creditors periodically reevaluate whether they offer or maintain covered accounts.

Establishment of an Identity Theft Prevention Program

Entities required to comply with the rule must establish a written identity theft prevention program ("**Program**") that is designed to detect, prevent

Definition of a Creditor

Creditor is defined in the FCRA as any person who, in the ordinary course of business:

- regularly extends, renews or continues credit, or any person who regularly arranges for the same;
- obtains or uses consumer reports, directly or indirectly, with a credit transaction;
- furnishes information to consumer reporting agencies in connection with a credit transaction; or
- who advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person.

Under the FCRA, the definition does *not include* a creditor who advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person.

and mitigate identity theft in connection with the opening and maintenance of covered accounts. The proposed rules require that financial institutions and creditors implement policies and procedures that are reasonably designed to:

- identify and incorporate red flags, defined as patterns, practices or activities that indicate the possible existence of identity theft, into any Program;
- detect the existence of red flags;
- appropriately respond to detected red flags in order to prevent and mitigate identity theft; and
- update any Program periodically to reflect changes in risks of identity theft to customers and to the safety and soundness of the financial institution or creditor.

The proposal allows financial institutions and creditors that already have existing policies and procedures in place to protect customers from identity theft to incorporate these existing policies and procedures into their Programs.

Identification of Red Flags

In addition to the proposed rule, the Commissions have issued guidelines that must be considered when implementing and administering any Program. These guidelines instruct financial institutions and creditors on how they can identify red flags by providing risk factors to be considered, as well as potential sources and categories of red flags. While all of the guidelines are not required to be incorporated into any Program, the proposal requires financial institutions and creditors to consider them during Program implementation.

Risk Factors

In the guidelines, the Commissions identified the following risk factors that financial institutions and creditors are required to consider when implementing a Program:

- the types of covered accounts they offer or maintain;
- the methods they provide to open covered accounts;
- the methods they provide to access covered accounts; and
- their previous experiences with identity theft.

Sources of Red Flags

The guidelines also provide that any Program should incorporate red flags from the following sources:

- prior experiences or incidences of identity theft;
- methods of identity theft used that reflect changes in identity theft risks; and
- applicable regulatory or supervisory guidance.

Select Examples of Red Flags by Category

Alerts, Notifications or Warnings from Consumer Reporting Agencies

- A consumer reporting agency provides notice of a credit freeze.
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual activity of an applicant or customer.

Suspicious Documents

- Documents presented appear to have been altered or forged.
- The photograph or physical description on identification provided do not match the appearance of the applicant or customer presenting the identification.

Suspicious Personal Identifying Information

- Personal identifying information, such as date of birth or social security number, is inconsistent when compared against external sources.
- Personal identifying information provided is of a type commonly associated with fraudulent activity, for example, the address is fictitious, or is a mail drop or a prison.
- The address or telephone number provided is the same or similar to addresses and telephone numbers submitted by an unusually large number of other persons opening accounts or other customers.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

- An institution receives a request for new means of access to an account shortly after a customer has changed the address on the account.
- A new revolving credit account is used in a manner commonly associated with known fraud (for example, for cash advances).

Categories of Red Flags

The Commissions have also identified various categories of red flags that financial institutions and creditors must consider including in any Program. These categories of red flags are:

- alerts, notifications or warnings received from consumer reporting agencies or services providers, including fraud detection services;
- presentation of suspicious documents;
- presentation of suspicious personal identifying information, such as address changes;
- any unusual use of, or suspicious activity related to, a covered account; and
- any notice received from customers, victims of identity theft or law-enforcement authorities in connection with a covered account.

The Commissions have provided examples of red flags, some of which are listed in the accompanying sidebar.

Detection of Red Flags

As part of their Programs, financial institutions and creditors are required to have policies and procedures in place to detect the presence of red flags in connection with the opening of new covered accounts and maintaining existing accounts.

For new accounts, financial institutions and creditors should obtain identifying information about the person opening the account, and should verify the identity of any new customer. For existing accounts, financial institutions and creditors should authenticate customers, monitor transactions, and verify the validity of any address changes submitted in connection with customers' accounts.

Responding to Detected Red Flags

The proposal requires that financial institutions and creditors implement policies and procedures to respond appropriately to any red flags that they have detected. The proposed guidelines state that an appropriate response will depend on the degree of risk posed by the detected red flag, and that aggravating factors which may heighten the risk of identity theft should be considered. Such aggravating factors may include, for example, unauthorized access to a customer's account records, or if the customer provides information related to his or her account to someone fraudulently claiming to represent the financial institution or creditor.

Updating the Program

The proposal also requires that Programs be updated periodically. Updates should be based on any changes in risks of identity theft to customers or to the safety and soundness of the financial institution.

Appropriate Responses to Detected Red Flags

The Commissions' guidelines provide examples of appropriate responses to detected red flags. An appropriate response may include:

- monitoring a covered account for evidence of identity theft;
- contacting the customer;
- changing passwords, security codes or other means of accessing customer accounts;
- opening an account with a new account number;
- not opening a new account;
- closing an account;
- not attempting to collect on a covered account or not selling a covered account to a debt collector;
- notifying law enforcement; or
- taking no action if it is determined that no response is warranted under the circumstances.

Factors that a financial institution or creditor may consider when updating its Program are:

- any prior experiences with identity theft;
- changes in methods of identity theft;
- changes in the detection, prevention or mitigation of identity theft;
- changes in the types of accounts it offers; and
- any changes in business arrangements, including mergers, acquisitions, alliances, joint ventures or service provider arrangements.

Administration of Programs

Senior-Level Oversight Required

The proposed rules require that either the board of directors or a committee of the board of directors approve the initial written Program. The board of directors, a committee of the board or a designated senior management level employee must also be involved in the oversight, development, implementation and administration of the Program.

Appropriate oversight of any Program must include:

- delegating responsibility for the Program's implementation;
- reviewing reports prepared by staff showing compliance with these rules; and
- approving material changes to the Program as necessary to identify risks of identity theft.

The continued administration of any Program must also include training staff as necessary for implementation, as well as the exercise of effective oversight of arrangements with service providers, as discussed in further detail below.

Reports Demonstrating Compliance with Programs

Effective administration of any Program requires that the staff responsible for developing, implementing and administering it provide reports at least annually of the financial institution or creditor's compliance with these rules. The reports must be furnished to the designated person or group charged with overseeing the Program.

These reports should include relevant information relating to the effectiveness of the policies and procedures in place in identifying and addressing the risk of identity theft, service provider arrangements, any significant incidents involving identity theft and management's response and any recommendations for material changes to the Program.

Oversight of Arrangements with Service Providers

The Commissions recognize in their proposing release that financial institutions and creditors may engage service providers to perform activities in connection with customer accounts. The proposed guidelines require that financial institutions and creditors take steps to ensure that these service providers employ reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft. The Commissions state that while service providers may have their own policies and procedures in place to address identity theft concerns, financial institutions and creditors are still responsible for ensuring that any service provider's program complies with the requirements of the rules.

Requirements for Card Issuers

The proposed rules also establish duties of financial institutions and creditors who issue credit or debit cards (card issuers) in connection with cardholder accounts. The joint proposal addresses obligations of card issuers with respect to cardholder changes of address by imposing a duty on card issuers to establish reasonable written policies and procedures to assess the validity of any request to change a cardholder's address for a credit or debit card account.

The proposed rules also require that if a card issuer receives a request to issue a replacement credit or debit card within at least the first 30 days following a request to change a cardholder's address, the card issuer must not issue a replacement card until it has:

- notified the cardholder of the request, and provided to the cardholder a reasonable means of promptly reporting incorrect address changes; or
- otherwise determined the change of address to be valid in accordance with the policies and procedures required under the rule.

Notifications must be sent to the cardholder's former address, or be provided by any other means of communication to which the cardholder and card issuer have previously agreed to. These notifications must be clear and conspicuous, and be provided separately from the card issuer's other correspondence.

As a practical matter, the Commissions note that there are very few entities under either agency's jurisdiction that issue credit or debit cards. In fact, in the release, the CFTC notes that it is unaware of any entities subject to its jurisdiction that offer credit or debit cards, and that some entities are expressly prohibited from doing so. Thus, it is likely that few financial institutions or creditors will actually be subject to the proposed card issuer rules.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Daniel N. Budofsky
212 450 4907
daniel.budofsky@davispolk.com

Gerard Citera
212 450 4881
gerard.citera@davispolk.com

Robert L.D. Colby
202 962 7121
robert.colby@davispolk.com

Susan C. Ervin
202 962 7141
susan.ervin@davispolk.com

Annette L. Nazareth
202 962 7075
annette.nazareth@davispolk.com

Lanny A. Schwartz
212 450 4174
lanny.schwartz@davispolk.com

Other Legal Requirements

Finally, the proposed guidelines state that financial institutions and creditors must be mindful to continue to comply with other legal requirements in addition to the proposed Identity Theft Red Flags Rules. For example, other requirements may address:

- the filing of Suspicious Activity Reports;
- circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;
- furnishing information to consumer reporting agencies; and
- prohibitions on the sale, transfer and placement for collection of debts resulting from identity theft.

Comment Deadline and Effective Date

The comment period on the proposed rules ends May 7, 2012. The Commissions have proposed that the Identity Theft Red Flags Rules become effective 30 days following the date that the final rule is published in the Federal Register.

© 2012 Davis Polk & Wardwell LLP

Notice: This publication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. If you would rather not receive these memoranda, please respond to this email and indicate that you would like to be removed from our distribution list. Please add Davis Polk to your Safe Senders list or add dpwmail@davispolk.com to your address book.