As published in ABA Risk and Compliance – September/October 2024

CrossCheckCompliance

FCRA Fundamentals

Consumer Alerts and Identity Theft

BY JOHN PACE, CRCM

Financial institutions (FIs) obtain sensitive information regarding consumer credit histories to determine the risk level of a consumer's request for deposit or credit accounts. Bad actors, through a variety of tactics and schemes, increasingly compromise consumer information through identity theft to impersonate consumers and obtain accounts illegally.

Consumers who have been the victim of identity theft have several options available to them to alert FIs that their credit information is vulnerable or has been compromised because of identity theft. Consumers may contact any of the three nationwide credit reporting agencies (CRAs) and place a fraud alert or freeze on their credit information. Similarly, to protect themselves proactively, military service members may place an Active-Duty alert with the CRAs to inform FIs that they have been called to active duty.

The Fair Credit Reporting Act (FCRA) requires that FIs create a written Identity Theft Prevention Program (ITPP) (16 CFR 681.1(d)(1)). The ITPP must be designed to identify, detect, and respond to "red flags," which are defined as patterns, practices, or specific activities that could indicate identity theft. FCRA details the types of accounts subject to the identity theft red flag rules (known as "covered accounts"), the types of alerts that a consumer may place with a CRA on a covered account, and categories of potential red flags with examples under each category. A clear understanding of these definitions and requirements will aid in building or enhancing an effective ITPP.

Covered Accounts

The FCRA Identity Theft Rules defines a "covered account" in two ways. First, as "an account that a financial institution offers to or maintains [for a person], primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions." Second, as "any other account that the financial institution … offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution … from identity theft, including financial, operational, compliance, reputation, or litigation risks." (16 CFR 681.1(b)(3))

Every FI must periodically determine whether it offers, or maintains in its portfolio, covered accounts (16 CFR 681.1(c)). Covered accounts

include deposit accounts, loans, lines of credit, and similar account types. A periodic compliance risk assessment should take into consideration the:

- Types of accounts the FI offers or maintains;
- Methods the FI provides to open accounts;
- Methods the FI provides to access the accounts; and
- Previous experiences the FI has had with identity theft.

In order to mitigate the risks associated with fraud and identity theft, FIs should develop a solid framework to identify, investigate, and resolve any red flags that arise during the creation or ongoing maintenance of accounts the FI has determined are subject to the FCRA Identity Theft Rules. This includes ensuring that employees have the knowledge to recognize alerts the FI receives related to potential identity theft.

Alerts, Freezes, or Warnings from a Credit Reporting Agency (CRA)

There are several ways that an FI may be alerted that a consumer has been the victim of identity theft. These alerts warn that a consumer's identity has been stolen, or is at risk due to active-duty status, and any new requests for credit in the consumer's name may be fraudulent. There is no charge for consumers to place fraud alerts on their accounts. The consumer will need to submit proof of identity so that the CRA is able to confirm the fraud alert request is valid. A consumer needs only to contact one of the three nationwide CRAs to place a fraud or active-duty alert. That CRA is required to share the alert with the other nationwide CRAs. There are three types of fraud alerts that a consumer may place with a CRA and the actions an FI must take to address the alert.

1. Initial Fraud Alert (IFA)—An FI must verify the consumer's identity prior to issuing credit in the consumer's name. An IFA is valid for one year.
2. Extended Fraud Alert (EFA)—This alert is like an IFA, except that an EFA is valid for seven years. To place an EFA, a consumer must prove that the proper authorities were notified of the fraud.
3. Active-Duty Alert—This alert is valid for one year and can help protect a consumer when deployed for active-duty military service. When an active-duty alert has been placed, an FI must verify the consumer's identity before issuing new credit in the service member's name.

While fraud alerts are a significant signal of potential identity theft, they are not the only avenues for CRAs to notify FIs of potential identity theft or fraud. Additional ways FIs may be alerted to potential fraud or identity theft include:

1. *Credit/security freeze;* A credit/security freeze does not mean that a consumer's identity has been stolen. It is a proactive measure by the consumer to restrict access to their credit report. A consumer has the option to temporarily lift the credit/security freeze when applying for new credit. FIs must work with the consumer to unfreeze their credit information.
2. *Notice of address discrepancy:* CRAs may also provide a notice of address discrepancy as part of a consumer report provided to an FI. This occurs when there is a substantial difference between the consumer's address provided by the FI to obtain the consumer report and the consumer address in the CRA's records. An FI must have reasonable

policies and procedures designed to enable the FI to form a reasonable conclusion that the consumer report relates to the subject consumer. (12 CFR 1022.82)

3. Unusual *Patterns of activity:* In addition to alerts or notifications from a CRA, unusual patterns of recent activity, when compared to the consumer's credit history and usual pattern of activity, may indicate potential identity theft or fraud. Some examples of unusual activity include, but are not limited to:
    - A recent, significant increase in the volume of inquiries;
    - An unusual number of recently established credit relationships;
    - A material change in the use of credit, especially with respect to recently established credit relationships; or
    - An account that was closed for cause or identified for abuse of account privileges by an FI.

Other Potential Identity Theft Red Flags

There are several other categories of red flags which FIs should watch for when originating a new account for a consumer. Examples include, but are not limited to:

Suspicious Documents

- Documents provided for identification that appear to have been altered or forged.
- A photograph or physical description on the identification is not consistent with the appearance of the applicant or consumer presenting the identification.
- Information on the identification is inconsistent with information provided by the applicant or consumer presenting the identification, or is inconsistent with readily accessible information the FI has on file such as a signature card or a recent check.
- An application appears to have been altered or forged or gives the impression of having been destroyed and reassembled.

Suspicious Personal Identifying Information (PII)

- The PII provided by the consumer is not consistent with external information sources, such as the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.
- The PII provided by the consumer is inconsistent with other identifying information.
- The PII provided is associated with known fraudulent activity as indicated by internal or third-party sources used by an FI.
- The type of PII is commonly associated with fraudulent activity, as indicated by internal or third-party sources used by an FI. Examples include the:
    - Address on the application is fictitious, a prison, or a mail drop (an address used only to receive letters and packages to be picked up later (not a Post office Box); or
    - Phone number is invalid or is associated with a pager or answering service.
- The SSN provided is the same as submitted by other consumers or other current customers.

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

- Soon after a change of address is requested by the consumer, the FI receives a request for a new, additional, or replacement card or for the addition of authorized user on an account.

- A new revolving credit account is used in a way that is like known patterns of fraud. For example, most or all of the available line is used for cash advances or merchandise which may be readily sold for cash.
- The use of an existing account has a change in use pattern that is inconsistent with past patterns of activity on an account, or an existing account that has been inactive for a lengthy period is used.
- Mail sent to a customer is returned repeatedly as undeliverable, while transactions continue to occur with the covered account.
- An FI is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft

One of the most obvious red flags is when an FI is notified by a customer, a victim of identity theft, the police or other law enforcement agency, or any other person that the FI has opened a fraudulent account for someone engaged in identity theft.

Designing an Effective Identity Theft Detection, Prevention, and Mitigation Program

What can an FI do to detect, prevent, and mitigate potential identity theft? Thankfully, the regulatory agencies have developed interagency guidelines for the creation of an ITPP. The guidelines establish five primary pillars of an effective ITPP.

Identifying Relevant Red Flags

There are three key areas FIs should include under this pillar to ensure identification of potential identity theft. First, an FI should incorporate into its ITPP and procedures all red flags relevant to its products and services under the categories discussed above. The interagency guidelines include examples under each category in Appendix A to 16 CFR 681. The examples are not all inclusive but are a good starting point. Second, FIs should consider and document risk factors for each of the relevant red flags it has identified. Third, FIs should identify the sources of relevant red flags, as described in the FCRA. Identification of all relevant red flags is foundational to building a strong ITPP.

Detecting Red Flags

Once an FI has determined the identity theft red flags relevant to its products and services, it must establish the framework for how red flags will be detected. The framework should be supported by comprehensive policies and procedures for opening covered accounts and periodic monitoring of existing covered accounts. For account opening, the FI's Customer Identification Program and related identity verification processes should be used as the basis for verifying the identity of consumers seeking an account. For existing accounts, periodically authenticating customers, monitoring account activity, and verifying the validity of address change requests are examples of detection processes for covered accounts.

Preventing and Mitigating Identity Theft

While identifying and detecting identity theft red flags are very important, neither matter much if an FI does not follow through on the information to prevent and mitigate identity theft. The ITPP policies and procedures should include appropriate responses for the red flag(s) detected. The responses should be based on the risk level of the red flag as established by the FI's ITPP. Examples of appropriate responses include, but are not limited to, contacting the customer, not opening a new covered account, closing an

existing covered account, or notifying law enforcement.

Updating the Program

Essential to maintaining an effective ITPP is a periodic review of the program to ensure it is up to date regarding risks to customers or to the safety and soundness of the FI, specifically losses due to fraud. Factors to consider include recent experiences of the FI with identity theft and changes in methods of identity theft. Making sure risk assessments and processes stay current is essential to the ITPP remaining effective.

Administration of the Program

As part of an effective compliance management program, an FI must establish effective oversight and administration of the ITPP. The board of directors (Board) or a committee of the Board should review and approve the initial written program and any subsequent updates or revisions. Adequate reporting on the program should be provided on a periodic basis to the Board. The frequency of reporting should be based on the risk profile for the program and the FI. Training should be provided to employees on the ITPP and the FCRA as it relates to the employees' roles in the organization, and there should be oversight of any third-party service providers who impact the FI's ITPP.

Regulatory Examination Considerations

Due to the high impact of identity theft to both consumers and FIs, the regulatory agencies pay special attention to ITPPs. To demonstrate to the agencies that an adequate program is in place, documentation is key. FIs should ensure that sufficient documentation is retained for risk assessments, identity verifications, red flag identification, detection processes, and actions taken related to identity theft. Reporting to the Board or delegated oversight committee should be comprehensive enough to keep the oversight body well informed but not overwhelm them with unnecessary details. Employees should be knowledgeable regarding identity verification and red flags related to identity theft. Employees should also be comfortable bringing forward identity theft concerns related to new or existing customer accounts.

By developing an understanding of what constitutes a red flag as related to identity theft and building an effective ITPP, FIs can protect themselves and their existing and prospective customers.

ABOUT THE AUTHOR

JOHN PACE, CRCM, is a manager at CrossCheck Compliance, LLC and a regulatory compliance and audit professional with over 20 years of experience in banking, mortgage banking, and as a regulator. Most recently, John was the director of regulatory change management at Freedom Mortgage. He has also held various audit roles at USAA and U.S. Bancorp. His career began at the Federal Reserve Bank of Minneapolis as a financial analyst and then an examiner, leading regulatory compliance examinations for state member banks. John can be reached at jpace@crosscheckcompliance.com.

ABA MEMBER RESOURCES

ABA Frontline Compliance Training: Fair Credit Reporting Act: aba.com/training-events/online-training/fair-credit-reporting-act-fcra