IDENTITY THEFT PREVENTION: HOW TO CATCH A THIEF

Jonathan Foxx, PhD, MBA
Chairman & Managing Director

Here are four scenarios involving identity theft that mortgage originators encounter from time to time. Read them and then keep them in mind as I discuss how to ask for additional information in order to prevent identity theft.

1. A law enforcement report containing detailed information about the identity theft and the signature, badge number, or other identification information of the individual law enforcement official taking the report should be sufficient on face value to support a victim's request.

   Question: Without an identifiable concern, such as an indication that the report was fraudulent, would it be reasonable for an information furnisher or Consumer Reporting Agency (CRA) to request additional information or documentation?

   Answer: It would not be reasonable.

2. A consumer might provide a law enforcement report similar to the above report, but certain important information such as the consumer's date of birth or Social Security number may be missing because the consumer chose not to provide it.

   Question: The information furnisher or CRA could accept this report, but would it be reasonable to require that the consumer provide the missing information?

   Answer: It would be reasonable.

3. A consumer might provide a law enforcement report generated by an automated system with a simple allegation that an identity theft occurred to support a request for a tradeline block or cessation of information furnishing.

   Question: Would it be reasonable for an information furnisher or CRA to ask that the consumer fill out and have notarized the Commission's ID Theft Affidavit or a similar form and provide some form of identification documentation?

   Answer: It would be reasonable.

4. A consumer might provide a law enforcement report generated by an automated system with a simple allegation that an identity theft occurred to support a request for an extended fraud alert.

    Question: Would it be reasonable for a consumer reporting agency to require additional documentation or information, such as a notarized affidavit?

    Answer: It would not be reasonable.

In these scenarios, a financial institution should be responsive in accordance with certain guidelines. Specificity of action must be appropriate, reasonable and proportional to the challenge. However, total reliance on the CRA is inappropriate.

Undertaking Evaluative Actions

In avoiding identity theft schemes, I suggest that four basic evaluative actions be undertaken, where a decision is needed to ask for additional information from the consumer.

1) Specific dates relating to the identity theft such as when the loss or theft of personal information occurred or when the fraud(s) using the personal information occurred, and how the consumer discovered or otherwise learned of the theft.
2) Identifying information or any other information about the perpetrator, if known.
3) Name(s) of information furnisher(s), account numbers, or other relevant account information related to the identity theft.
4) Any other information known to the consumer about the identity theft.

When a financial institution is faced with declining a loan for identity theft, a report should be drafted with relevant information to support the decision. Simply declining a loan and issuing an Adverse Action disclosure or alleging identity theft by reporting it to Financial Crimes Enforcement Network (FinCEN) by filing a Suspicious Activity Report (SAR) is not sufficient. Regulators and internal auditors routinely ask for an identity theft report in order to determine the extent to which an investigation was conducted. Furthermore, such an investigation demonstrates the institution's "good faith" commitment to its Anti-Money Laundering Program, "good faith" being a key demonstrative element in a regulator's assessment of the institution's compliance. Other regulations are triggered, too, such as those promulgated by the Federal Trade Commission in its Identity Theft Protection Program as well as the regulations of the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA), which is an amendment to the FCRA, primarily to protect consumers against identity theft.

Identity Theft Report

The identity theft report should consist of the following components:

- The allegation of identity theft with as much specificity as the consumer can provide.
- A copy of an official, valid report filed by the consumer with a federal, state, or local law enforcement agency, and even the United States Postal Inspection Service.[1]
- Additional information or documentation that an information furnisher or consumer reporting agency reasonably requests for the purpose of determining the validity of the alleged identity theft, provided that the information furnisher or consumer reporting agency:
    - Makes the request not later than 15 days after the date of receipt of the copy of the identity theft report form or the request by the consumer for the particular service, whichever will be the later.
    - Makes any supplemental requests for information or documentation and final determination on the acceptance of the identity theft report within another 15 days after its initial request for information or documentation.

- Has 5 days to make a final determination on the acceptance of the identity theft report, in the event that the consumer reporting agency or information furnisher receives any such additional information or documentation on the 11th day or later within the 15-day period.

Understanding Identity Theft

But what is identity theft? Over time, this concept has gone through ever wider definitions.

I propose a simple outline, helpfully provided by the FACTA.[2]

> Identity theft means a fraud committed or attempted using the identifying information of another person without authority.

This seems straight-forward and unambiguous.

However, the term "identifying information" leads to a more nuanced definition, because that terms means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

- Name, Social Security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, or routing code; and,
- Telecommunication identifying information or access device.

Naturally, the process of determining what constitutes appropriate proof of identity is pivotal in making a decision about the presence or absence of identity theft. Consumer reporting agencies are usually at the forefront of finding ways to establish identity, in that they are required to develop and implement reasonable factors involving the information that consumers must provide to constitute proof of identity.[3]

These factors must:

- Ensure that the information is sufficient to enable the CRA to match consumers with their files; and,
- Adjust the information to be commensurate with an identifiable risk of harm arising from misidentifying the consumer.

Identity Theft Alerts

When Lenders Compliance Group conducts a due diligence review, my firm's auditors evaluate the choice of information that our client considers to be reasonable information for proof of identity.

One factor is what we call the "consumer file match," which is the identification information of the consumer, including his or her full name (first, middle initial, last, suffix), any other or previously used names, current and/or recent full address (street number and name, apt. no., city, state, and zip code), full nine digits of Social Security number, and/or date of birth.

Another factor we call "additional proof of identity," which usually consists of copies of government-issued identification documents, utility bills, and/or other methods of authentication of a person's identity (which may include, but would not be limited to, answering questions to which only the consumer might be expected to know the answer).

Additionally, it is critical to determine if the consumer has placed a fraud alert on the consumer report. The two alerts that are required by CRAs to place on consumer reports are fraud alerts and the active duty alerts.[4]

A fraud alert is a notice that the consumer may have been a victim of identity theft or other fraud.

An active duty alert is a notice that the consumer is on active duty in the military.

There are timing requirements.[5] An initial fraud alert must be placed in a consumer's report for ninety (90) days at the consumer's request. If the consumer files an identity theft report, an extended fraud alert can remain in the consumer's report for seven (7) years. An active duty alert will remain in the consumer's report for twelve (12) months.

The initial fraud alert and active duty alert notify all prospective users of the consumer report that the consumer does not authorize the establishment of any new credit plan, increase in credit limit on an existing credit account, or other extension of credit (other than under an existing open-end credit plan), in the name of the consumer, or issuance of an additional card on an existing credit account requested by a consumer unless the lender follows the required procedures.

If an initial fraud alert or active duty alert appears on a consumer report, a lender cannot extend credit unless the user utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request. These policies and procedures can be a heavy lift and often need competent compliance guidance to navigate.

If a consumer requesting the alert has specified a telephone number to be used for identity verification purposes, before authorizing any new credit plan or extension in the name of the consumer, the lender must contact the consumer using that telephone number or take reasonable steps to verify the consumer's identity and confirm that the application for a new credit plan is not the result of identity theft.

Additionally, there is the "extended fraud alert," where the consumer's report must include information that provides all prospective users of the consumer report with:

- Notification that the consumer does not authorize the establishment of any new credit plan or extension of credit (other than under an existing limit of an open-end credit plan) in the name of the consumer, or issuance of an additional card on an existing credit account requested by a consumer, or any increase in credit limit on an existing credit account requested by a consumer, unless the lender first contacts the consumer as specified in the report, and
- A telephone number or other reasonable contact method designated by the consumer for lenders to contact the consumer to verify their identity.

Extended fraud alerts prohibit lenders from establishing a new credit plan or extension of credit (other than under an existing limit of an open-end credit plan) in the name of the consumer. A financial institution may not issue an additional card on an existing credit account requested by a consumer, or increase credit limit on an existing credit account requested by a consumer, unless the company contacts the consumer in person or uses the contact method described in the consumer report to confirm that the application for a new credit plan or increase in credit limit, or request for an additional card is not the result of identity theft.

SCAMMERS WILL BE SCAMMERS

But scammers always scam and conmen always con. Conman is the short form for "Confidence Man," because such an individual has a knack for gaining a mark's confidence and then pulling the scam which, in this case, is stealing the mark's identity. A financial institution or other business entity that provides credit to an identity thief (or other person who allegedly has made unauthorized use of a victim's identification) must provide a copy of the application and other records it has (or are maintained by another on the business entity's behalf) regarding the transaction (i.e., copies of checks or card sales slips).[6] The victim's request must be in writing, contain certain information, and be mailed to an address specified by the business entity for this purpose.

Intent is important in identifying and nailing the scammer, because the victim is a consumer whose means of identification or financial information has been used or transferred (or has been alleged to have been used or transferred) without the authority of that consumer*, with the intent to commit, or to aid or abet, an identity theft or a similar crime.*

Where such identity theft has been determined, the financial institution – and any other business entity that has provided credit based on allegedly unauthorized use of the means of identification of the victim – must provide a copy of the application and business transaction records in its control,[7] evidencing any transaction alleged to be a result of identity theft to:

- The victim;
- Any federal, state, or local government law enforcement agency or officer specified by the victim in such a request; and,
- Any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of identity theft records under this provision.

There is an important caveat: the applicable rule does not permit a company to disclose information, including information to law enforcement, that it is otherwise prohibited from disclosing under any other provision of federal or state law. That being said, the law also specifically states that the privacy provisions of the Gramm-Leach-Bliley Act (GLBA) prohibiting the disclosure of financial information by the company to third parties cannot be used to deny disclosure of the required information to the victim.

VICTIM REQUESTS

There are three parts involved in a financial institution's handling of a victim's request for a report. These are basic features of identity theft prevention compliance. The three parts are the rules involving the victim's request requirements, the response provided to the victim, and the action(s) taken by the financial institution.

Firstly, telephonic requests must be avoided. The request of a victim for copies of identity-theft-related records must be in writing and be mailed to an address specified by the financial institution, if any. During this phase, the financial institution can ask for additional information from the consumer as part of the request. If asked, the consumer can be required to include relevant information about any transaction alleged to be a result of identity theft to facilitate providing the records including, if known by the victim (or if readily obtainable by the victim), such information as the date of the application or transaction and any other identifying information such as an account or transaction number.

Secondly, when the institution does receive such a request from the consumer, it must provide the information within thirty (30) days of receiving the request. The information must be provided free to the consumer, with no charges. However, before providing the information, the company must first verify the identity of the consumer making the request. If there is a high degree of confidence that it has satisfactorily established the identity of the victim making the request, it may then respond by providing the information.

Caution in this phrase is critical! As a matter of the institution's review process, and prior to releasing the requested information, the victim should be expected to provide proof of identity with:

- The presentation of a government-issued identification card;
- Personally identifying information of the same type that was provided to the company by the unauthorized person; or
- Personally identifying information that the institution typically requests from new applicants or for new transactions, at the time of the victim's request for information, including any of the above documentation.

For establishing the claim of identity theft, the victim should provide:

- A copy of a police report evidencing the claim of the victim of identity theft; and

- A properly completed copy of a standardized affidavit of identity theft developed and made available by the Commission or an affidavit of fact that is acceptable to the business entity for that purpose.

Thirdly, the action(s) taken are the next hurdle. The institution may decide to decline providing the requested information if, in good faith, it determines that:

- The FCRA does not require disclosure of the information;
- After reviewing the information provided by the consumer to verify their identity, the company does not have a high degree of confidence in knowing the true identity of the individual requesting the information;
- The request for the information is based on a misrepresentation of fact by the individual requesting the information relevant to the request for information; or
- The information requested is Internet navigational data or similar information about a person's visit to a web site or online service.

BLOCKING INFORMATION

There are rules involving the blocking of information involving identity theft.[8] For instance, CRAs must block the reporting of any information in the file of a consumer that the consumer identifies as information which resulted from an alleged identity theft, not later than four (4) business days after the date of receipt by the CRA of:

- Appropriate proof of the identity of the consumer,
- A copy of an identity theft report,
- The identification of such information by the consumer, and
- A statement by the consumer that the information is not information relating to any transaction by the consumer.

In our audit reviews, Lenders Compliance Group determines if the CRAs comply with applicable regulations by their prompt furnishing of appropriate information related to findings of identity theft, proper filing of an identity theft report, and whether a block has been requested and, if so, the effective dates of the block.

CONSUMER RIGHTS

Finally, I would like to call attention to the summary of rights of identity theft victims.[9] The FTC, in consultation with the federal banking agencies and the National Credit Union Administration (NCUA), created a model summary of the rights of consumers that is to be provided to consumers by CRAs for remedying the effects of fraud or identity theft involving credit, an electronic fund transfer, or an account or transaction at or with a financial institution or other creditor. In addition, the FTC revised its *General Summary of Consumer Rights* under the FCRA because of the numerous changes to consumer rights made by the FACT Act.[10]

The *Summary of Consumer Identity Theft Rights*[11] essentially highlights consumers' rights in the FACT Act and other FCRA provisions and must be provided by CRAs to consumers who contact them claiming to be the victims of identity theft. The revised *General Summary of Consumer Rights*[12] is required to be provided by CRAs to all consumers when they receive various disclosures from CRAs.

---

[1] Such a filing often subjects the person filing the report to criminal penalties relating to the filing of false information, if, in fact, the information in the report is false.
[2] 12 CFR 1022.3. The Federal Trade Commission (FTC) adopted several definitions of terms that are used in a number of provisions of the FACT Act.
[3] 12 CFR 1022.123. See also 605A, 605B, and 609(a)(1) of the Fair Credit Report Act (FCRA)
[4] Under section 605A of the FCRA, as added by section 112 of the FACT Act

[5] Idem
[6] Under section 609(e) of the FCRA, added by section 151 of the FACT Act
[7] Whether maintained by the business entity or by another person on behalf of the business entity. The basis of the allegation involves the culpability provided in inducing a financial institution or other business entity the consideration of products, goods, or services to, accepting payment from, or otherwise entering into a commercial transaction with a person who has allegedly made an unauthorized use of the victim's identity.
[8] Under section 605B of the FCRA, added by section 154 of the FACT Act
[9] Section 609(d) of the FCRA sets forth requirements for the model summary.
[10] Required by section 609(c) of the FCRA
[11] See Appendix I to 12 CFR Part 1022
[12] Under the FCRA appears in Appendix K to 12 CFR Part 1022

LENDERS COMPLIANCE GROUP®

The first mortgage risk management firms in the United States that provides professional guidance and support to financial institutions, banks and nonbanks, in virtually all areas of mortgage banking.

Pioneer in residential mortgage compliance, mortgage risk management, and regulatory guidance.

Contact

Compliance@LendersComplianceGroup.com.

Media

Media@LendersComplianceGroup.com.

Phone

866-602-6660

Lenders Compliance Group | Brokers Compliance Group | Servicers Compliance Group | Vendors Compliance Group | LCG Quality Control