
■ ■ ■

Identity Theft Fraud: Effects and Preventive Measures for the Lending Institution

Megan Finneran

St. Edward's University

We typically think of identity theft fraud as a crime that victimizes the individual whose personal information has been stolen. However, identity theft and the related fraudulent uses of that information cause significant problems for lenders as well. According to Ahern (2003) identity theft has been the most prevalent and fastest growing crime in the United States. In addition to the harm done to individuals, lenders stand to experience significant losses and liabilities in connection with identity theft fraud. Security protocols, including the use of fraud protection software products and application verification systems, can protect lenders and their consumers from some of these adverse effects. Lenders should acknowledge the danger that identity theft poses and take action to prevent fraud from occurring in their institutions.

Identity theft is a crime in which the perpetrator steals and uses another individual's personal information (such as Social Security number or account numbers) for fraudulent purposes. In 1998, Congress passed the Identity Theft and Assumption Act, making identity theft a Federal crime. The Act identifies identity theft as a crime in which one does the following:

Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. (U.S. Congress, 1998, p. 1)

For the purposes of this law, personal information includes Social Security number, account numbers, credit card numbers, or any information that can be used to identify an individual (U.S. Department of Justice, 2000). This stolen information is used to remove money from the account of the identity theft victim or to create a new loan or account in that person's name. The consumers have traditionally been identified as the victims of these crimes. However, lenders are affected by a need to protect both their consumers and themselves from financial losses and legal liability (Krebsbach, 2004).

Lenders, as well as consumers, suffer financial losses due to identity theft fraud. The Towergroup analysts have estimated that lenders incur between \$1 and \$3 billion in losses each year from identity theft fraud. This is a conservative estimate, as it does not take into account application or document fraud. Pratt surveyed 60 banks and found that almost 1% of bank account and credit card applications are fraudulent, and the average loss for a fraud transaction is \$6,795 (as cited in Krebsbach, 2004, p. 23). Although many lenders have fraud insurance, increasing instances of fraud can drive these costs up, as well as scare potential customers away.

Lenders must protect their customers from identity theft in order to protect themselves from liability. The Fair and Accurate Credit Transaction Act of 2003 has placed some of the responsibility for protecting consumer information on the lender. Lenders must now verify

address change requests and abbreviate account numbers when they are printed. (U.S. Congress, 2003) Failure to comply is a violation of Federal law, and leaves the lending institution open to penalties. Additional steps to safeguard consumer information are in the best interest of the lender. A lender could be implicated in a fraud if it does not take adequate measures to ensure consumer information is secure, because this lack of security could be considered aiding or abetting under the Identity Theft and Assumption Act (U.S. Congress, 1998). Shredding all documents containing consumer personal information is an important security measure. Some perpetrators can obtain all the information they need to commit fraud by simply looking through the dumpsters behind banks and other lending institutions (Venetis, 2002).

Antifraud software, services, and procedures are needed to combat the increasing fraud rate. Traditional security measures have proven to be insufficient. New procedures and tools must be used to prevent identity theft fraud at all levels. Lenders are already aware of one type of identity theft fraud: transaction fraud. Transaction fraud occurs when an unauthorized individual removes funds from an existing bank account, line of credit, or credit card. Software products are appearing on the market to screen accounts for suspicious transactions, flag them, and then alert staff to verify the authenticity of these transactions to prevent further fraud on that account. Monarch, an antifraud product from Datawatch, operates in this way. Employee accounts, accounts that have numerous deposits over \$5,000, and accounts that have a large number of significant wire transfer activity would be flagged for inspection by this program (Songini, 2004). Using software programs like these, many lenders are successfully stopping defrauders from continued abuses on single accounts. However, this type of prevention occurs later in the process by identifying fraud once it has occurred and only preventing further fraud on that same account (Krebsbach, 2004).

Other types of fraud leave traces earlier in the process and require a different sort of screening for prevention. Application fraud is a growing area that lenders find more difficult to detect and prevent. Application fraud occurs when stolen personal identification information is used to open a new loan or account (Krebsbach, 2004). This type of fraud can occur when a perpetrator opens an account in another person's name, or alters supporting documents to create a loan in his or her own name. By using computer technology, criminals can alter their own pay stubs, tax returns, and bank statements. They can also place their

names on documents that have been stolen from legitimate consumers (Venetis, 2002). Traditionally, lending risk managers have scrutinized credit card applications for possible fraud. Many lenders were not prepared when an increase in mortgage and other collateralized loan fraud began ("Potential for fraud abuse," 2004). One cannot just freeze a mortgage loan that is on the books like one can freeze a credit card account. At this point the lender's collateral is in the hands of an unknown person. Collections activity and the resources needed to find the collateral and the individual will cause additional costs ("Potential for fraud abuse," 2004). To be effective, document and application fraud must be caught before the application is approved.

Verification of applicant information, whether done by loan officers or fraud prevention service providers, is an essential step in stopping fraudulent applications from being approved. Fraud prevention services are one set of tools that lenders can use to weed out fraudulent applications in the underwriting stage. Service providers, such as eFraud and FraudFinder, review and score applications and supporting documents that are submitted for loans. The applications are scored to reflect the likelihood of fraud. A score indicating a high possibility of fraud would be given to an application if it had a high number of alert factors. Some alert factors these services look for are a high number of credit report inquiries, returned checks, or closed accounts. Address checks are done to verify the authenticity of the addresses on the application. Warm addresses (locations that are not likely to be residences) such as post office boxes, hotels, prisons, and business addresses are indicative of possible fraud. Addresses are checked to make sure that the zip codes, cities, and phone numbers correlate. Any discrepancies could indicate a mistake made when creating a falsified document (Venetis, 2002).

Verification of applicant information is essential to preventing fraud at the underwriting level. Using an external service provider to screen applications for fraud is helpful, but those lenders who do not want to incur the associated expenses can modify internal procedures to achieve similar results. Before approving a loan application, loan officers can take a few steps to verify that the person who submitted the application is the same person whose name and personal information appear on that application. Using free internet people finders, the loan officer can look up the address on the application to verify that the name and phone number at that address match. A follow up call to that number to verify that that individual has placed an application with the lender is another precautionary measure. With business

loans, it is important to verify with business owners that the person applying for loans and making transactions is authorized to do so. Often, lenders allow fraud to pass undetected by making dangerous assumptions that all information presented by an individual is correct, or that the individual is entrusted by his business to be applying for credit in the company name (Krebsbach, 2004). Even if other fraud detection methods are used, verification of applicant information is an important step in protecting one's lending institution from identity theft fraud.

The effects of identity theft fraud on the lending institution are serious: increased insurance rates, scandals that can scare away potential consumers, legal liabilities, increased collection costs, and direct losses through charge-offs. Lenders must recognize the potential for loss and liability caused by fraud at the information security,

transaction, and application levels. By taking precautions to protect consumers' personal identification information, lending institutions can thwart information thieves from obtaining the information they need to commit identity theft fraud. Fraud protection software is available to alert employees of suspicious transactions and to stop fraud from continuing once it has begun. The most overlooked fraud area, application fraud, is perhaps the most dangerous for the lending institution. While fraud protection providers are one way of preventing this type of fraud, it is essential that the loan officer take verification steps to authenticate applications and supporting documents. As the incidences of identity theft and fraud increase, preventive measures become even more vital to the continued success and health of the lending institution.

References

- Ahern, R. (2003, July/August). Managing credit and application fraud risks in a volatile economy: Technology is key. *Business Credit*, 105, 54-55.
- Krebsbach, K. (2004, April). Banks count losses as fraud numbers climb. *U.S. Banker*, 114, 22-24.
- Potential for fraud in noncard portfolios is being overlooked. (2004, September). *Credit Union Journal*, 8, 9.
- Songini, M. (2004, June). Fraud sniffers. *Computerworld*, 38, 42.
- United States Congress. (2003, June 26). *H.R. 2622 Fair and accurate credit transactions act of 2003*. Retrieved September 29, 2004, from <http://financialservices.house.gov/media/pdf/108hr2622ai.pdf>
- United States Congress. (1998, October 30). *Identity theft and assumption deterrence act of 1998*. Retrieved September 29, 2004, from <http://www.ftc.gov/os/statutes/itada/itadact.htm>
- United States Department of Justice. (2000, June 5). *Identity theft and fraud*. Retrieved September 29, 2004, from <http://www.usdoj.gov/criminal/fraud/idtheft.html>
- Venetis, K. (2002, September). Document fraud proves costly to lenders, consumers. *Mortgage Servicing News*, 6, 9.

Biography

Megan Finneran is an MBA student in the School of Management and Business at St. Edward's University. She received a BA in Sociology from Boston University. She is currently a manager for an outsourced collections group in Austin.