Best practices for preventing fraud losses and protecting customers from identity theft

Executive summary

"The biggest risk to an institution is not the consumer whose identity has been verified; it is the individual whose true identity is unknown." Meridian Research, Inc.[1]

"Know your customers" always has been important for preventing fraud and identity theft, which continue to become more sophisticated and widespread. Today, as government-enforced identification programs and other regulations proliferate, there are even more compelling reasons for knowing who your customers are. Given the growth of identity theft and greater concern for national security, industry experts believe more legislation to prevent economic crimes is likely soon.

Although most financial institutions already perform some type of verification as part of their customer identification and application process, they may not be doing enough to pass muster in today's business environment. Many experts feel that the industry is vulnerable and must take immediate action to review and revise current processes. This must take place in an atmosphere of concern for consumer privacy rights, an issue that has become even more sensitive in this new regulatory era.

At the same time, financial fraud is changing, necessitating a new approach to avoid losses and protect consumers. According to the Federal Trade Commission (FTC), identity theft is escalating at 40 percent a year, with much more damaging, long-term consequences for businesses and consumers than garden-variety transaction fraud. Federal agencies note that the vast majority of fraud now occurs at the point of origination through falsification of application information.

The good news is that by strengthening verification procedures, institutions will be less exposed to fraud losses — especially if verification is part of a more comprehensive fraud program. To successfully detect and prevent fraud, Experian® and other industry experts advise a more in-depth approach compared to standard credit risk assessment:

- Incorporate more information into the decisioning process, especially for high-dollar unsecured transactions.
- Break away from conventional thinking. Traditional credit scoring and underwriting procedures don't identify fraudulent applications.
- Dig deeper to verify identity beyond using Social Security numbers or other single pieces of data.
- Look for and assess the fraud potential of inconsistencies among all of the data available, not just in address and credit bureau information.

The right tools and processes, combined with quality data and fraud expertise, reduce fraud losses and protect consumers from identity theft and other fraud while preserving a positive customer experience. At the same time, using industry best practices for fraud prevention will help companies comply with government regulations. As financial institutions become more proactive and sophisticated in preventing fraud, there will be less need for additional regulation.

Fraud's reach: background and statistics

Financial fraud is one of America's largest growth industries, creating annual losses of $189 billion, according to Meridian Research, Inc. The cost of application fraud alone is more than $35 billion a year.[2] Far more damaging than delinquent or bankrupt accounts, fraud losses are generally three times higher than normal charge-off rates, posing a real and constant threat to profitability and raising the price of goods and services for all consumers.

By far the greatest threats come from e-commerce fraud, identity theft and international criminal organizations, all of which are becoming more widespread and sophisticated every day. The Gartner Group reports that online fraud is 12 times more likely than offline fraud.[3] Online merchants estimate that 5 percent to 6 percent of their transactions are fraudulent.[4] As e-commerce continues to grow, it will become an even bigger attraction for criminals.

According to the FTC, identity theft is escalating at 40 percent a year and is particularly problematic compared with more traditional forms of financial fraud. Greater access to credit, an abundance of information, faster electronic communications and intense competition among financial institutions make it easier than ever for perpetrators to steal identities and falsify information.

Called "one of the most insidious forms of white collar crime" by the U.S. Department of Justice, identity theft tends to be more damaging to both consumers and institutions. It typically results in multiple instances of fraud, which are often of higher dollar value than other types of fraud.

Identity theft is estimated to claim 100,000 victims a year, according to the FTC and the Consumer Data Industry Association. The economic and emotional loss to consumers is staggering. It may take as long as several years to restore a victim's credit reputation, and in the meantime financial and job opportunities may be lost. According to FTC estimates, the average identity theft victim doesn't discover the problem for 13 months and then invests an average of $1,173 and 175 hours attempting to repair his or her credit record.[5]

By its very nature, identity theft is more difficult to detect at the point of transaction than other types of financial fraud. By assuming an innocent consumer's identity, criminals can conduct transactions that appear legitimate. Fraud prevention programs must be able to stop identity fraud where it starts — at the point of application.

Application fraud losses rarely are recovered and are estimated to be $170 for every U.S. credit user every year.[6] Some industries, such as wireless telecommunications, auto financing and mortgage lending, are particularly attractive targets, with annual fraud losses in the United States estimated in the billions. Fraud losses to retailers and bankcard issuers are more difficult to calculate because they are often recorded as bad debt charge-offs. Even if only 1 percent of credit obligations are lost to fraud, this could total several billion dollars for just a few of the large bankcard issuers.

Current and pending legislation

"The USA PATRIOT Act is not a short-term solution, but a new way of doing business. In fact, we expect compliance requirements to grow in the future as the federal government identifies new threats [and] determines that existing applications are not working as desired."
Giga Information Group[7]

The growth of financial fraud in general — and identity theft in particular — has been accompanied by increasing antifraud legislation at both the federal and the state level. Industry analysts expect this trend to continue as heightened national security issues add a new dimension to the regulatory picture.

Legislation to prevent identity theft has been largely consumer-driven. Unlike other types of fraud, identity theft is especially damaging to consumers. Although they may not be held accountable for unauthorized purchases, they feel personally violated and spend significant time and effort restoring their credit reputations. Identity theft is now the number one fraud complaint reported by consumers to the FTC.

The following federal legislation now in force addresses identity theft and related national security concerns:[8]

- The Identity Theft and Assumption Deterrence Act (1998) defines identity theft and makes it a felony. However, because identity theft is often very complex and part of a whole pattern of other crimes, this Act has led to very few prosecutions.

- The Enhanced Border Security and Visa Entry Reform Act of 2002 tightens regulations governing entry and exit documents issued to aliens and requires the inclusion of unique biometric identifiers in all travel documents.

- The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intersect and Obstruct Terrorism) expands the scope of the Bank Secrecy Act (BSA) and the Office of Foreign Assets Control (OFAC). Section 326 requires that financial institutions establish a conforming Customer Identification Program (CIP) to verify the identity of anyone seeking to open an account and determine whether the person appears on federal government lists of known or suspected terrorists.

- In addition to federal legislation, nearly all states have passed some form of identity theft statute since 1996. However, many of them are ineffective because of limited resources and the fact that financial crimes often occur across state lines.

Pending federal legislation includes The Privacy Act of 2003, which would give consumers more control over how their personal information is used and provide a national standard for protecting Social Security numbers and other personal information from public dissemination. The proposed Social Security Number Misuse Prevention Act would restrict the use and display of Social Security numbers and establish criminal penalties for misuse.

Other proposed legislation would aid identity theft victims, increase penalties for identity theft and create a new category of aggravated identity theft to cover associated crimes.

Although most financial institutions may already perform some type of customer verification as part of their application process, they may not be doing enough to comply with current and pending fraud protection requirements. By strengthening verification procedures, institutions also will be less exposed to fraud losses — especially if verification is part of a more comprehensive fraud program. The right tools and processes, combined with quality data and fraud expertise, can help safeguard businesses from fraud losses and protect consumers from identity theft while preserving a positive customer experience. Furthermore, if financial institutions become more proactive in their approach to fraud prevention, the less likely the need for additional legislation.

Best practices for fraud prevention

"While preventing the processing of fraudulent transactions is certainly a valid and necessary endeavor, clearly today's financial system is replete with many more opportunities for criminals to commit fraud than ever before. Financial institutions must stop fraud at other points in the supply chain, particularly at the account opening or credit application stage." Meridian Research, Inc.[9]

Constant vigilance by businesses and consumers is needed to protect identities from theft or misuse. This is essential in managing fraud risk, but it is only the beginning. A vital key to success is differentiating fraud risk from credit risk.

Financial institutions are typically focused on credit risk and have a broad array of tools for assessing a consumer's ability to pay. Fraud risk — the likelihood that a consumer is who he or she claims to be — is the inverse of credit risk. Even if the same data sources are used, fraud risk analysis takes a different perspective on an applicant's information.

To successfully detect and prevent fraud, Experian and its financial analysts advise a more in-depth approach compared to standard credit risk assessment:

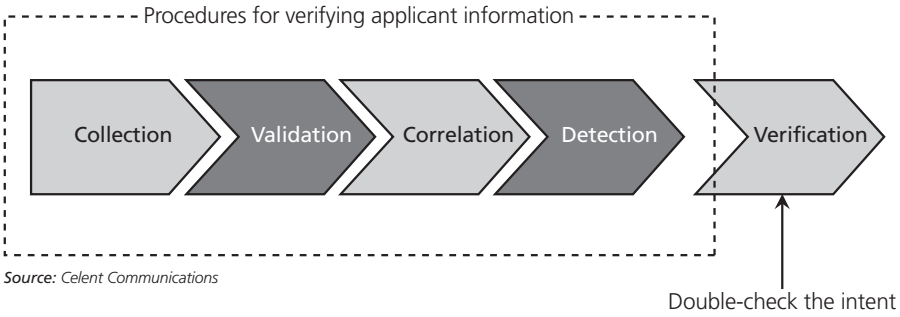
- *Incorporate more information into the decisioning process.* The responsible use of data is the most powerful weapon against fraud. Ideally, a 360-degree view of an applicant is desirable, especially for high-dollar unsecured transactions.

- *Break away from conventional thinking.* Traditional credit scoring and underwriting procedures don't identify fraudulent applications. A person's ability to pay has little bearing on whether he or she is potentially fraudulent.

- *Dig deeper.* Verifying identity using Social Security numbers or other single pieces of data is insufficient — especially for online transactions, which are much more vulnerable to fraud.

- *Look for inconsistencies and assess their fraud potential.* Verification processes should check for inconsistencies in all of the data available, not just in address and credit bureau information. Does the phone number go with the address? Do the age and Social Security number match? More checks provide a better assessment of fraud risk.

Since most identity theft fraud occurs at the application stage, this is the place to concentrate the most effort. A sequence of five procedures provides a progression of best practices for precautionary measures when opening accounts, as shown below:[10]



Source: *Celent Communications*

1. *Collecting data*
   Applications must require complete data, which can be used to identify the individual during the approval process.

2. *Validating data*
   Since personal IDs are unreliable for verifying identity, application data must be validated against credit reports and other trusted third-party sources.

3. *Correlating data*
   This process compares various pieces of data with other data on the application, looking for inconsistencies such as an address that does not match the phone number.

4. *Detecting fraud patterns*
   This essential step looks for typical fraud patterns within the application and among third-party information sources. Recently opened credit accounts under the same Social Security number but different names would be a red flag, suggesting a need for further manual review.

5. *Verifying the new account*
   Additional verification to confirm or double-check the individual's intent in opening the account is the final precautionary measure for which various methods can be used.

Evaluating fraud and compliance solutions

No single tool can provide the highest confidence in verifying customer identities. The optimal approach is integrating several different types of antifraud tools into a comprehensive solution, customized for a company's risk exposure, type of account, sales channels and other factors.

The foundation for any fraud prevention program is customer authentication — confirming that the person is who he or she claims to be. Because driver's licenses and other official government identification are so easy to falsify today, they are not sufficient verification unless the consumer is known to the institution and is conducting the transaction in person. This type of verification is referred to as documentary verification.

Nondocumentary verification, which can be used in addition to or instead of documentary verification, is essential to prevent fraud and is the basis for consumer authentication, especially in online or call center transactions. Nondocumentary verification includes:

- *Positive verification:* comparing information provided by the consumer with a trusted third-party source, such as a consumer reporting agency
- *Logical verification:* using commercially available analysis tools to determine the consistency of information from various sources
- *Negative verification:* checking information provided by the consumer against databases of known fraud, bad checks and government lists

Best practices integrate some or all of these techniques, as appropriate to a company's products, sales channels and risk exposure.

Positive verification
This is essential, especially for online, real-time transactions where the customer expects a fast, seamless experience. Technology that incorporates a reliable consumer database with several levels of authentication provides the most flexibility and confidence. The most basic level should use credit report data to verify name, address, phone number, Social Security number, date of birth and driver's license number. Preferably, this should include the option of incorporating a score based on matching algorithms to determine the likelihood of true identity. At the highest level, authentication should provide information for a customized, interactive session with the applicant, drawing on various databases for top-of-mind questions that only the true customer can answer.

Logical verification
Going beyond authentication to search for potential fraud, logical verification may be as simple as a series of searches, checks and counters with the customer's inquiry address and Social Security number as the critical identifiers. For even closer scrutiny, best practices use robust matching logic to compare a consumer's application with past applications, fraud records and credit data to create an all-around view of the applicant.

By revealing inconsistencies, anomalies and known fraudulent information, this approach can indicate identity theft and other fraud with much more precision than the more traditional approach of checking only name, address and Social Security number. It also should distinguish between fraud and credit risk. Instantaneous application matching deters criminals from submitting multiple applications on the same day and ultimately makes it more difficult for them to operate anonymously.

Negative verification
As a complement to positive and logical verification, negative verification provides a greater level of confidence by comparing consumer-provided information against databases of known fraud, bad checks and government lists. This type of data sharing is the first line of defense against identity theft and other financial fraud, a best practice that has only recently become available in a meaningful way in the United States. Data sharing illuminates patterns of fraud across industries, prevents reoccurrences and helps prosecute perpetrators.

There are many fraud products and services provided by an array of vendors, necessitating a thorough evaluation before deciding on the right approach for a particular financial services provider.

The most effective fraud solutions are comprehensive and incorporate best practices with the following factors:

- A synthesis of extensive data resources, advanced technology and fraud prevention expertise that can detect the simplest to the most complex kinds of fraud in all channels
- Based on trusted data sources that are deep, broad and unimpeachable and able to instantly deliver accurate data that is as up to date as possible
- In compliance with Fair Credit Reporting Act and other requirements to protect consumer privacy
- Real-time systems capable of fast response times (ideally under two seconds for authentication) for instant decisioning without any rekeying of data
- Customizable, with enough flexibility to support an organization's specific policies and procedures
- Modular and scalable to accommodate an institution's growth and changing needs as well as an increasingly regulated environment
- Easily implemented and integrated into a company's existing technology and procedures, without the need for retooling call centers or e-commerce Web sites
- Designed to provide a positive customer experience in all channels and ensure confidence in the company's efforts to protect customers from fraud
- Provided by a reliable, sizable vendor with extensive authentication and antifraud expertise that will be there to provide future support and upgrades

Experian: an innovative, integrated approach

"Many of our fraud prevention tools are used as standard industry best practice by financial institutions. The common link among all of our tools is their ability to help clients understand who it is they are dealing with so they can stop fraud before it starts."

Chris Callero, president, Experian's Credit Services

Innovation is the hallmark of effective fraud solutions, an essential part of staying ahead of a new breed of high-tech criminals who are increasingly more sophisticated and organized. As the thought leader and world leader in information solutions, Experian meets this challenge by continuing to invest in the development of new tools and techniques that raise the bar of effective fraud prevention. At the same time, the company stays abreast of changing antifraud legislation to provide the industry with solutions that are timely and compliant.

Experian's fraud scoring expertise, vast relational consumer database and comprehensive fraud prevention tools create a powerful defense for credit card issuers and processors, lending institutions, telecommunications companies, e-commerce businesses and retailers. Now, with the integration of an automatic OFAC list checking service in its verification tools, Experian offers solutions to help companies strengthen their Customer Identification Programs and comply with Section 326 of the USA PATRIOT Act.

As the developer of the most comprehensive and predictive fraud tools on the market, Experian has deep credentials based on a 30-year history of decision support and analytical expertise. A nationally recognized leader in fraud solutions, Experian is a trusted provider of quality data on 215 million American consumers and 25 million businesses.

As the industry's best-in-class provider of fraud solutions, Experian continues to pioneer new fraud prevention technologies and data sharing to identify fraud patterns across industries. Its end-to-end solutions bring together best practices for balancing customer convenience, privacy protection and fraud prevention to help institutions prevent losses and comply with government regulations.

Experian's extensive suite of fraud solutions focuses on fraud where it begins, with the application process. This includes:

- A range of powerful front-end application verification and authentication tools to verify that customer information is valid and to enable fast, confident decisions
- Government list checking service to help comply with Section 326 of the USA PATRIOT Act
- Credit-qualifying solutions to uncover potential fraud, compare inconsistencies on credit reports and check against a unique, proprietary cross-industry database of verified fraud records
- A decision engine for approving, declining or referring applications for manual review

Experian's fraud tools can be used independently or together, based on a company's procedures, the type of account being opened and the origination channel. Driven by advanced, unique technologies, our comprehensive approach to fraud prevention also provides many secondary benefits for clients. In addition to controlling fraud losses, companies can improve operational efficiency, lower account acquisition costs and increase account approval rates while reducing risk.

Sources

[1] ID Verification Solutions, Meridian Research, Inc., July 3, 2002

[2] Experian-commissioned study, 1997

[3] Businesswire.com quotes a July 2000 Gartner Group survey

[4] Anon.com quotes a December 1999 CyberSource report on fraud

[5] Identity Theft Resource Center of San Diego

[6] "Identity Thieves," TIME magazine, Feb. 11, 2002, Julie Rawe

[7] New Compliance Requirements for Financial Transactions, Giga Information Group, Oct. 10, 2002

[8] Financial Identity Theft: Prevention and Consumer Assistance, BITS Financial Services Roundtable, May 2003

[9] ID Verification Solutions, Meridian Research, Inc., July 3, 2002

[10] Taking a Bite Out of Credit Card Fraud, Celent Communications, January 2003, Ariana-Michele Moore