

How Financial Institutions Can Overcome Identity Theft Challenges

The increase of identity theft among financial institution customers, and federal requirements, such as regulations under the USA PATRIOT Act, have led banks, credit card companies and mortgage lenders to seek solutions that improve identity verification and reduce account takeovers. Identity theft directly impacts profits and the public perception of financial institutions. How can financial organizations adequately screen new accounts for fraud, authenticate existing customers and meet federal regulations? The answer lies in fraud prevention systems that perform intelligent, multi-sourced data analysis, returning single scores that determine the level of certainty that consumers are who they claim to be.

Identity Theft: The Modern Faceless Crime

Modern technology has made identity theft a crime that can be performed quickly and anonymously. Face-to-face business transactions of previous eras have been replaced with electronic transactions, call centers and mail-in forms, making it harder to catch criminals. In the world of financial services, identity theft typically involves attempts to take over accounts and access funds or credit lines using another individual's identification information. Additionally, fraud crimes involve efforts to establish new accounts under fraudulent or fictitious identities.

Identity theft is a crime that can be performed quickly and anonymously.

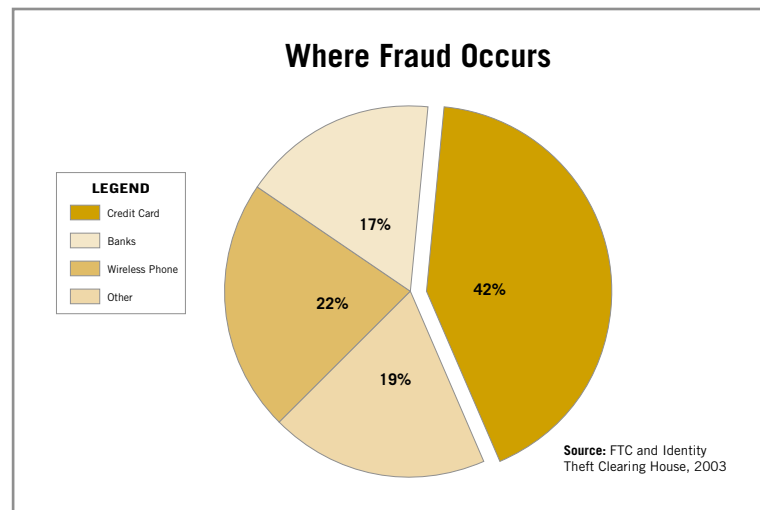
Access to information is the fraud perpetrator's chief weapon. The Internet has made it easy for criminals to acquire consumer information such as credit card numbers, Social Security numbers, names, addresses and birth dates. Additionally, fraud criminals can open new accounts online and gain control of existing accounts quickly, repeatedly and with little fear of prosecution. Smart financial institutions are beginning to attack this problem with new technology that validates identities by going beyond the normal methods of verification and authentication.

The Size of the Identity Theft Problem

Nearly one in eight adults in the U.S. has experienced identity theft at a cost to businesses and consumers of \$50 billion in 2002 alone (Federal Trade Commission, 9/2003). Of all complaints reported to the FTC, identity theft is the most common. The size of the identity theft problem is most likely understated because many victims never report the crime to local or federal authorities.

Almost two-thirds of all identity theft claims in 2002 involved financial service organization customers.

Credit card and bank fraud accounted for 59 percent of all identity theft claims in 2002 (FTC, 2003—see chart below). Each stolen identity results in an average of \$17,000 in fraudulent charges or losses (Identity Theft Resource Center). Most banks consider identity fraud the largest threat against their deposit accounts (American Bankers Association 2002 industry survey).



Often financial institutions do not become aware of identity fraud until after losses have occurred, and consumers may not realize their identity has been stolen until much later. A solution is needed that can help prevent imposters from taking over accounts or establishing false accounts.

Fraud Implications for Financial Institutions

Financial institutions face numerous challenges as a result of identity fraud abuses. Issues range from turning down good customers who fail fraud screenings to the negative perception that financial institutions are not doing enough to protect consumers. Consider the following challenges:

- **Opportunity cost:** If credit applicants are improperly screened for fraud when establishing new accounts, legitimate new customers may fail the fraud screening process. These false-positive results lead to lost opportunities for financial services organizations.
- **People cost:** Investigating and manually reviewing potential frauds and false-positive results are expensive, labor-intensive processes.

- **Financial losses:** A significant amount of profit is lost to fraud. By not controlling fraud, financial institutions often need to initiate or raise annual fees and increase interest rates.
- **Poor customer service:** Too many, or poorly articulated, identity-related questions equate to a negative customer experience, while the wrong types of questions lead customers to wonder about the security of their information.
- **Consumer convenience:** Convenience and ease of transacting are a growing part of the value equation among customers. Financial organizations need to avoid offending customers with overly intrusive authentication requests.
- **Public perceptions:** Financial institutions must overcome the public perception that they are not doing enough to protect consumers from identity theft.
- **Compliance:** The USA PATRIOT Act requires that financial institutions reasonably confirm that a consumer who is opening an account is who he or she claims to be.

Identity Verification: A Historical Perspective

In the 1980s, financial institutions had very basic validation checks that could verify whether Social Security numbers were valid and not issued to deceased persons. In addition, addresses and phone numbers that were involved in previous cases of fraud were flagged as suspicious.

Social Security numbers became such a common form of identification that many states used them on driver's licenses and some businesses used them as account numbers.

In the 1980s, simple Social Security number verification systems were the only method of confirming identities.

The rationale was that Social Security numbers could be used as a universal form of identification. However, the common use of Social Security numbers, combined with the growing popularity of the Internet and electronic commerce, made it easier for criminals to acquire them.

In recent years, state and federal legislation have called for the elimination of Social Security numbers as account numbers and driver's license numbers. In addition, state legislation has called for no disclosure of Social Security numbers on printed, published or posted documents.

In the 1990s, identities were validated by determining if items such as a Social Security number and a birth date were consistent. Systems could also match ZIP Codes with telephone area codes to determine if an application was valid. By the late 1990s, many aspects of a person's identity (such as name, address, phone number and Social Security number) could be verified using a third-party database.

In the early 2000s, systems were developed that leveraged customer data integration technology to bring multiple aspects of a person's identity together from many sources. Issues such as changes of address, marriage name changes and divorces could quickly be validated to reduce false-positive rates.

Today, multiple external databases can combine in- and out-of-wallet information to provide a greater level of validation. For example, questions such as "What was your previous address?" can be asked for authentication purposes. Using modern analytic tools, systems can also determine if a Social Security number was mistyped. These modern solutions intelligently analyze multiple sources of data to accurately predict the likelihood of fraud. The future involves access to new and improved databases to better verify and authenticate customers.

Today's Solution: Intelligent Fraud Prevention Systems

To adequately prevent account takeovers and the opening of fraudulent accounts, financial organizations need a fraud prevention system that performs intelligent data

Intelligent fraud prevention systems use multiple sources of data to provide a score that predicts the likelihood of fraud.

analysis about individuals using information from multiple sources. Performing customer information analysis from multiple sources enables financial organizations to better determine if an individual is a fraud, meet federal regulations and reduce false-positive rates in a single integrated offering. An intelligent fraud prevention system quickly produces a score that indicates the likelihood of fraud. These real-time systems help financial institutions make smarter decisions, process customers and prospects faster, lower manual processes and reduce overall fraud losses.

An intelligent fraud prevention system examines "in-wallet" and "out-of-wallet" information. In-wallet information includes items typically found in a person's wallet, such as his or her name, address and Social Security number. Out-of-wallet information includes facts a customer knows but a criminal would find harder to access. Out-of-wallet information could include how many years the customer lived at his or her current address and his or her employer.

Financial companies have been slow to adopt new fraud prevention solutions because the technology is perceived as very expensive. However, modern systems are more cost-effective and can quickly provide a return on investment by reducing fraud.

An intelligent fraud system can provide:

- **Identity verification:** Determines the validity of applicant information and searches databases to determine the likelihood the application is a fraud.
- **Identity authentication:** Provides an interactive presentation of challenge questions combined with an evaluation of responses to confirm that a customer is who he or she claims to be.
- **Investigation tools:** Offers interactive tools that enable a financial institution to perform identity research about individuals.
- **Compliance:** Provides database searches that assist with compliance with the USA PATRIOT Act and other federal identity requirements.

Benefits of Multi-Sourced Data Analysis

Intelligent fraud prevention systems leverage multiple external sources of data and apply analytical techniques to improve fraud detection accuracy and broaden the scope of understanding about a financial customer or applicant. Specific benefits include:

Offers Greater Accuracy

Multi-sourced systems provide a broader and deeper picture of a person to help financial institutions better screen for fraud. By leveraging and linking databases

Multi-sourced fraud prevention systems offer greater accuracy and validation while reducing false-positive rates.

such as phone directories, driver's license files, credit data, voter registration information, warranty registrations and magazine subscriptions, a financial institution can better validate a person's identity. This is especially important for applicants with little or no credit history, such as students or recent immigrants.

By verifying the identities of these audiences, financial institutions have access to new market opportunities.

Provides Better Validation

A multi-sourced solution reduces the risk of containing incorrect or out-of-date information. Single-sourced solutions, however, are often based on self-proclaimed user reports. Consider an imposter who takes over an account and changes an address on file for a credit card holder. A multi-sourced system can verify an address change with many other sources simultaneously, serving as a powerful fraud deterrent.

For those opening new accounts, many aspects of information can be verified with a greater level of assurance. For example, an address can be checked to see if it is valid or if it belongs to a postal box, commercial mail receiving agency (CMRA), hospital or

prison. A phone number can be verified as affiliated with the address provided and checked to see if it is a mobile number. A Social Security number can be checked to see if it was issued before or after the applicant's birth, if it belongs to another individual or if the applicant is utilizing multiple Social Security numbers. Out-of-wallet questions can also be used to further verify an applicant.

A multi-sourced solution can also find inconsistencies or unique patterns that might indicate fraud. By locating inconsistencies, financial institutions can better deter fraud.

Lowers False-Positive Rates

Better up-front validation lowers a financial institution's risk of fraud. The net result is increased profitability from reduced fraud write-offs. In addition, the customer experience is enhanced as real customers are properly verified in real time.

What to Look for in an Intelligent Fraud Prevention System

When deciding on an intelligent fraud prevention system, a number of requirements must be adequately addressed:

- **Solution flexibility:** Fraud patterns tend to change, and a fraud prevention solution must adapt to changes. The ability to look to a variety of new, frequently updated databases and calculate different fraud scores without costly updates is critical. In addition, the solution should be flexible enough to adjust by line of business, channel and geographic parameters.
- **Open access and integration:** A solution must integrate easily into existing financial systems while remaining open to future data input. As new data sources become available and financial systems change, the solution must be able to access new data while integrating with any system.
- **True analytics:** The solution should objectively determine what constitutes fraud rather than relying on error-prone subjective scoring.
- **Multi-sourced data:** To provide a thorough picture of a person's identity, many sources must be examined and analyzed in a historical context.
- **Federal compliance:** The solution should assist with compliance of federal regulations such as the USA PATRIOT Act, which may include accessing special government databases.
- **Processing options:** The solution should provide a variety of options for producing a fraud score, ranging from real time to overnight batch operations.

- **Breadth of data sourcing:** A solution should access government and private-sector databases from many sources nationwide. Solutions should not be limited to consortium-only data sources.
- **Fraud and risk analysis:** Powerful solutions integrate fraud risk scores and fraud analysis into a single unified inquiry.
- **Recognized leader:** Be sure to work with a recognized leader in the fraud analysis space. Often these leaders offer one-stop solutions for verification, authentication and compliance requirements, making it easier to implement and maintain solutions.

The Acxiom and TransUnion Solution—Fraud Management Platform

Acxiom and TransUnion have come together to create the industry's most comprehensive, intelligent fraud prevention solution. Designed to significantly reduce

The Fraud Management Platform offers multi-sourced data access, analytics and decision-based fraud prevention.

fraud loss for financial organizations, the Acxiom and TransUnion Fraud Management Platform (FMP) combines multi-sourced data access with analytic and decision-based software to provide a highly accurate fraud indicator. The FMP meets all of the important requirements identified as critical features of an intelligent fraud prevention system.

The FMP reduces fraud losses by enabling financial organizations to strengthen their identity verification processes. Using multiple sources to verify and authenticate identities, the FMP reduces the likelihood of account takeover and helps identify fraudulent applications. FMP is a data-rich solution that incorporates business intelligence, robust analytics and decisioning into a flexible platform that can dramatically reduce false-positive rates. FMP also provides fraud investigation tools as well tools to assist with compliance with the USA PATRIOT Act.

FMP provides the following benefits:

- Reduces fraud loss via improved identity verification.
- Increases opportunities and reduces false-positive rates via highly accurate identity verification.
- Provides compliance assistance with the USA PATRIOT Act.
- Enhances customer experience through a less intrusive and highly accurate verification system.

The FMP offers the following important advantages:

Highly Flexible Solution

The FMP enables the creation of customized fraud scores so financial organizations can create scores that change as their needs change. Internal company data can be combined with the FMP to further customize the solution. FMP can also display specific identity inconsistencies.

Open Access and Integration

FMP works with existing systems common in financial organizations and is not intrusive to existing platforms. In addition, FMP supports standard protocols and is adaptable to all types and formats of data used in the financial industry. Acxiom and TransUnion also provide support staff to help financial organizations identify strategies, set analytic capabilities and create customized settings.

True Analytics

The FMP provides two options for analyzing fraud: a fraud score and custom decisioning. The fraud score is a simple number generated in response to an applicant's identification information. The score indicates the likelihood of fraud and can be used to trigger an investigation or challenge questions. The FMP fraud score is based on a comprehensive model developed by extensively analyzing fraud cases in the financial services industry utilizing the latest neural net technology. Custom decisioning enables financial institutions to modify score formulas for specific customer segments or channels, facilitating an enhanced decisioning process. In addition, FMP can identify inconsistencies with Social Security numbers, indicating an error was involved in the application. Moreover, phonetic and spelling errors (such as Kathy versus Cathy), aliases and maiden names can all be determined or corrected.

FMP provides an objective analysis of fraud by returning a simple fraud score.

Extensive Multi-sourced Data

The FMP utilizes more than 60 databases, providing the most comprehensive identity analysis in the industry. Data sources are constantly updated and FMP provides historical context of an individual's identity. Common application information is cross-checked with many data sources to identify inconsistencies. Both in-wallet and out-of-wallet data are analyzed for a tiered verification and authentication process.

Federal Compliance

The FMP aids in compliance with Section 326 of the USA PATRIOT Act by enabling data-driven identity verification of customers and applicants. FMP also can record that the financial organization inquired about an account holder's identity when the account was opened, and provide a domicile street address for each applicant (including those using a P.O. Box or CMRA).

Many Processing Options

FMP is flexible enough to work in Internet, call center, kiosk and walk-up environments, and also provides real-time access, multiple batch operations and desktop analysis.

FMP provides real-time access and batch operations for a variety of applications.

Real-time access is ideal for point-of-sale applications, call centers and Internet applications. Batch operations are helpful for processing mail-based applications. Desktop analysis enables investigators to perform powerful searches and respond to fraud events.

Streamlining Risk Analysis Processes

The FMP data verification results can be used to streamline creditworthiness risk analysis systems so operators do not need to re-key information to request both fraud and risk scores. For example, when an application is entered into FMP, a fraud score is generated. If the score indicates fraud is unlikely, the application is forwarded to risk decisioning. If a fraud score falls within the fraud parameters, a set of challenge questions is generated. If those questions are answered correctly, the application continues to creditworthiness risk decisioning. If the questions are answered incorrectly, further investigation may be necessary.

Recognized Leader

Together, Acxiom and TransUnion have extensive data integration and fraud analysis experience. Acxiom has been a leading data decisioning expert for more than 30 years, and TransUnion has delivered fraud management solutions for nearly a decade. The FMP is a one-stop solution for identity verification, authentication, research and compliance requirements.

Why Acxiom and TransUnion?

Acxiom's extensive data integration and management expertise coupled with its formidable data intelligence background make it an ideal partner in a joint fraud solution. TransUnion is a leading global information solutions corporation that provides business intelligence, analytics and commerce services to leading businesses worldwide. The company's extensive knowledge of consumer and risk data is strengthened by robust analytical abilities. Together, Acxiom and TransUnion have created a unique fraud offering, utilizing their data resources, technology, customer data integration, recognition, analytics and consulting to offer a single, powerful, intelligent fraud prevention solution. The FMP is a complete solution for identity verification, authentication, research and compliance requirements.

Acxiom and TransUnion have extensive expertise in the financial services market. Five of the top 6 retail banks and 13 of the top 15 credit card issuers rely on Acxiom and TransUnion for services. Additionally, both organizations have unparalleled reputations for customer service.

To find out more about the Acxiom and TransUnion Fraud Management Platform, visit www.acxiom.com or www.transunion.com.

Axiom Corporation • #1 Information Way • P.O. Box 8180 • Little Rock, AR 72203-8180
1.501.342.4221 • www.axiom.com

AXIOM



TransUnion • 555 West Adams Street • Chicago, IL 60661
www.transunion.com