White Paper

Combating Identity Fraud: An Overview of Complementary Approaches

Identity fraud demands constantly evolving prevention strategies to thwart ever-shifting criminals.

February 2010

LexisNexis®

Risk Solutions
Financial Services

Introduction

Identity theft is an old crime—it's been around at least since Jacob stole Esau's inheritance and Aesop's wolf slipped into something a little more comfortable to snatch an easy meal. In the digital age, however, computers and global data integration enable identity fraud on an unprecedented scale. We have seen reports of identity theft schemes of incredible scope and cunning, including one fraud ring that involved at least 20 conspirators working together to steal the credit histories of more than 30,000 people.[1]

In 2003, the FTC reported that nearly 10 million Americans discovered they were the victim of some form of identity theft in the previous year.[2] While an individual whose information is misused bears a small percentage of the cost of identity theft, victims estimate they had spent on average $500 and 30 hours to resolve the problem.[2] Victims of "new account" identity theft spend even more time and money—on average 60 hours resolving the problem with $1,200 average spend. This time, money and stress to the consumer often comes from fraud that happened in only one day.[3]

Identity theft hurts businesses as well. The FTC reports identity theft losses to businesses and financial institutions total nearly $48 billion. For all forms of identity theft, the loss to business was $4,800 per instance, but new accounts opening losses reach over $10,000 per instance.[4]

Identity theft is not only a financial problem. The use of false identifiers and false documents is intertwined with terrorism and many criminal activities, including drug trafficking, alien smuggling and money laundering. Organized criminal enterprises exploit weak or non-existent identity verification systems to fund their organizations, hide money and cross borders with impunity.

Solutions

Preventing identity fraud requires an efficient and reliable means of verifying an individual's identity. In general, there are three basic approaches: **trusted token, biometrics** and **knowledge-based processes.**

1. A **token-based** system recognizes an individual by his possession of an official identifying item, such as a driver's license, passport or national identity card. Each of these "tokens" bears a description of the person that presumably would not match an imposter. The weaknesses of this system are that tokens are easily replicated or stolen.

2. The developing field of **biometrics** is the second means of human identification. It relies on the recognition of some individualized individual characteristics (e.g., fingerprints or retinal scanning).

Modern identity fraud is one of the greatest challenges facing governments, corporations and financial institutions. LexisNexis® has been a leader in the study of identity fraud and in the development of automated solutions to combat it. Through its participation in identity fraud reports[5], law enforcement-private sector meetings and conferences and in industry-sponsored identity fraud events, LexisNexis has assumed an industry leadership position in the fight against this insidious menace.

The strength of the biometric approach is that everyone has uniquely identifying physical characteristics. The weakness of this system is that it can be easy to mismatch a name with a biometric or even to steal a biometric, thus incorrectly verifying an identity. Because biometric technology is still underdeveloped, these systems are expensive to implement. Biometrics remains an evolving technology best combined with other types of identity solutions to be effective.

3. Finally, **knowledge-based** systems rely on the matching of personally identifying data with information provided by a new customer or applicant. The process is generally referred to as identity authentication if it involves the use of identifying information like name, address and Social Security number. The institution quickly checks this information (usually through a third-party data provider) before commencing business with the individual. Identity authentication applications can also be enhanced through a "dialogue" process. In verifying an individual's identity, the institution will ask questions to which only the "real" owner of that identity could know the answers (e.g., color and model of the applicant's previous car, if a relative lives in a specific state, etc).

Each of the above identity verification methods are important tools in the fight against identity theft; however, the application of each can vary. For example, handprint verification can be an effective way to control access to an important building, but it's not a feasible method for a bank to verify new customers at the point of account opening.

When the individual to be identified is completely unknown to the verifier, knowledge-based identity authentication is the best solution because without previous information on which to build, an entity will not be able to know that John Doe really is who he says he is. Utilizing a biometric or token-based system in this case, without first authenticating an individual, simply provides an opportunity for an imposter to link a false name or other false identifiers with that individual's biometrics or token. This initial phase in the establishment of an identity management phase, referred to as identity proofing, is undoubtedly the most difficult identification problem facing any institution and is highly dependent on a knowledge-based system of identity verification.

Knowledge-based identity theft: A deeper explanation

As described above, the authentication process uses independent business or consumer data to verify the person or company with which the entity will conduct business. Sophisticated identity authentication tools use personally identifying information that is time sensitive, such as past and present address and phone numbers; dates of birth, marriage or death (an imposter may not realize the false identity is actually that of a deceased individual);

LexisNexis® InstantID® and LexisNexis® InstantID® Q&A are examples of knowledge-based authentication solutions.

or "out-of-wallet" information such as information about a previous car or previous residence. Databases are searched to verify the information provided by the customer. The data is analyzed using judgmental or empirical scoring models designed to identify highly suspicious or contradictory findings, which have a high propensity of being the result of identity theft. After the data is analyzed, a score or index is developed to organize the data in categories for efficient decision making. The score or index is a high-level summarization of results and categorizes the levels of identity theft risk. The scoring process can also take into consideration the lack of some information to verify identity. This identity authentication process works for both face-to-face transactions and internet or phone transactions (i.e. where the consumer and the credit card are not physically available.)

Because identity theft perpetrators can adapt quickly, identity authentication tools must constantly be examined and improved to defeat attempts to "game" the system and identify emerging practices. Also, the required level of authentication varies by use. For example, what may be required to authenticate a person applying for a mobile phone will differ from the authentication required of a person opening a bank account. Decision makers can use the scores or indices provided by authentication models to develop account-opening procedures and policies to ensure consistent business decisions on new accounts.

Identity authentication in the real world

Section 326 of the "USA PATRIOT Act" 31 USCS § 5318(l), passed by Congress after the September 11 terrorist attacks, highlights the crucial national security role for identity authentication. The Act's final regulations require banks and other financial institutions to verify the identities of all new customers, through the development of risk-based Customer Identification Programs.

There are numerous ways to construct a solid Customer Identification Program and most include some type of automated system. Because identity thieves are getting more sophisticated, technologies need to constantly evolve to stay ahead of the latest identity theft patterns. Identity authentication products need to perform several functions to be effective, most notably they should validate data by determining if the data exists (e.g. is the address real, does the phone number exist, etc.) and verify data by determining if the data all belongs together.

Identity authentication processes should also identify the presence of any high-risk conditions. Certain factors have proven to indicate a higher risk of identity theft than others (e.g. an address is a mail drop, motel, campground or prison). By understanding those risk factors, a determination can be made as to the level of risk in account applicants.

Identity authentication products—such as InstantID—offered by LexisNexis and exclusively endorsed by the American Bankers Association (ABA) help financial institutions comply with new account opening procedures.

Identity authentication products such as InstantID—offered by LexisNexis and exclusively endorsed by the American Bankers Association—help financial institutions comply with these new account opening procedures. InstantID verifies information across multiple databases and validates information such as name, address, date of birth and Social Security number, while identifying potentially high-risk data elements.

LexisNexis policy-based information sharing solutions

As noted throughout this paper, identity theft prevention solutions require verifying information comprised largely of personally identifiable information. The challenge for LexisNexis is to collect, aggregate and disseminate the requisite verifying information, while simultaneously protecting privacy. LexisNexis meets this two-fold purpose through policy-based information sharing, consisting of the following:

First, use of certain LexisNexis data is governed not only by existing laws such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act, but also by an industry-leading Data Privacy Policy that LexisNexis has established. Data privacy issues are studied by an established Privacy Policy Board, under the oversight of a chief privacy officer.

Second, LexisNexis continually strives to embed privacy enhancements into its information sharing technologies. An example of privacy enhancement technology is InstantID, which limits the personally identifiable information delivered to the customer to an identity authentication index and a narrowly crafted explanation, thereby achieving identity verification and data proportionality.

Third, LexisNexis works with its customers to address the policy issues affecting their use of verifying information, so that the financial institution receives the appropriate solution to appropriately address its fraud, terrorism financing and money laundering risk, while simultaneously protecting the privacy rights of its customers.

Conclusion

The individuals who commit identity theft present an ever-shifting target. Their motivations range from greed to fanaticism, but in the end they have but one goal—to achieve some unlawful objective while appearing to be someone else. A variety of tools, including biometrics and token-based systems, will be needed to combat the many forms of identity theft; however, a knowledge-based identity authentication system will continue to be an instrumental way to verify a person's identity. Growing trust in the identity authentication process will help nations protect their borders, facilitate global commerce, stop terrorists in their tracks and protect citizens from criminals stealing their lives.

Sources

[1] News Conference on Huge Identity Theft Case, Transcript # 112501CN.V00. CNN, November 25, 2002.

[2] Federal Trade Commission, Identity Theft Survey Report, September 2003.

[3] Ibid.

[4] Ibid.

[5] Gordon, Dr. Gary R. and Norman A. Willox, Jr. Identity Fraud: A Critical National and Global Threat, October 28, 2003, < www.lexisnexis.com/presscenter/hottopics/ECIReportFINAL.pdf.>

For more information:

Call 866.858.7246 or visit lexisnexis.com/risk/financial-services

About LexisNexis® Risk Solutions
LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.