

Underreporting of Identity Theft Rewards the Thieves

Some 7 million U.S. adults were identity theft victims during the past 12 months, according to new Gartner research. Because the crime is often misclassified, the thieves have a one out of 700 chance of being caught.

Core Topic

Financial Services: Financial Services
Architectures and Emerging Technologies

Key Issue

What architecture models and technologies will enable FSPs to adapt to major industry trends such as straight-through processing, the real-time enterprise, corporate performance measurement and risk management?

During the past year, 3.4 percent of U.S. consumers — 7 million adults — were victimized by identity theft, according to a Gartner survey of more than 2,400 adults conducted in May 2003. However, only 5,807 arrests were made by the FBI, Secret Service and U.S. Postal Service in 2000, the last year of available full-year data. Data from 2001 does not show a notable increase; however, even if it is assumed that arrests nearly doubled to 10,000 during the past year (which is highly unlikely), the criminals still have a one out of 700 chance of getting caught by federal authorities.

Identity theft is not necessarily a high-tech crime, and can just as easily damage the credit reputations of low-tech adults who don't spend any time on the Internet. More than half of all identity theft is committed by criminals who have established relationships with their victims, such as family members, roommates, neighbors or co-workers, according to U.S. Federal Trade Commission (FTC) documentation of identity theft cases where the method of theft was known, or 20 percent of the 94,100 identity theft complaints the FTC received between November 1999 and October 2001.

Identity theft is distinct from payment or credit card fraud, where transactions are fraudulently committed with a stolen bank card or account. During the past year, 5.5 percent of U.S. adults, or more than 11 million consumers, were victimized by credit card fraud, according to the new Gartner survey. With identity theft, a thief takes over a consumer's entire identity by stealing critical private information (such as Social Security number, driver's license number, address, credit card number or bank account number) so that the thief can use the stolen information to obtain illegal loans or credit lines to buy goods and services under the stolen name. Identity thieves typically change the consumer's mailing address to hide their activities.

Gartner

© 2003 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Identity theft is a heinous crime; it can take victims many years to restore their wrongfully damaged credit reputation. According to the FTC, most victims don't even know that their identities were stolen until an average of 13 months later, when it's typically too late to catch the perpetrator — who has typically stopped using the identity long before. Aside from ruining the victim's credit reputation, making it very difficult for him or her to obtain new loans or credit cards, it takes a victim approximately 175 hours to attempt to correct his/her credit records, according to industry sources.

Why Such a Large Disconnect Between Thefts and Arrests?

Banks, credit card issuers, cell phone service providers and other enterprises that extend financial credit to consumers — industries that thieves typically target to illegally obtain credit so they can buy goods or services under the stolen name — don't even recognize most identity theft fraud for what it is. Instead, they mistakenly write it off as credit losses when the thieves — whom they don't recognize as thieves — don't pay their bills. Hence, there is a serious disconnect between the magnitude of identity theft that innocent consumers experience and industry's proper recognition of the crime. This creates a disincentive to fix the problem with the urgency it requires.

Credit-extending enterprises keep reserves on their balance sheets for credit and loan losses. Increasing loan-loss reserves can eventually damage an enterprise's standing in the financial markets, so public companies try not to let their losses swing out of control. In contrast, identity theft fraud is directly expensed, but most enterprises only recognize a small percentage (probably 20 percent) of the fraud resulting from identity theft. The rest is incorrectly classified as a credit loss when the thieves don't pay their bills.

Fraud rates are generally between 0.25 percent and a little more than 0.5 percent of all credit application transactions, according to industry sources. Non-face-to-face transactions, such as instant credit offered online or cell phone service sold over the telephone, have the highest fraud rates. However, even in those sectors, most of the damage is misclassified as a credit loss because the thief doesn't pay the bill. ID Analytics, one of the vendors offering an identity-theft-prevention solution, claims that, according to its analysis of 200 million client customer records, up to 70 percent of identity-theft fraud is misclassified as credit loss. In the cell phone industry and other non-face-to-face lending environments — the hardest hit sectors — the 0.5 percent fraud rate rises to between 6 percent and 8 percent if the identity theft fraud is tagged properly, according to ID Analytics.

Does misclassification of the crime sound unfair to the consumer? It is. However, the incentives for the industry to fix the problem are not nearly strong enough, although some legislators are gradually trying to change that. Still, legislative and regulatory measures will take years to mature and become effective. In the meantime, identity theft continues to rise, according to consumer surveys done by the Bankers Roundtable Technology Secretariat (BITS), which consists of the nation's largest financial institutions. Other industry observers estimate that identity theft incidents rose 72 percent between 2001 and 2002.

Preventing Identity Theft Fraud

Without external pressure from legislators and industry associations, financial services providers (FSPs) may not have sufficient incentive to stem the flow of identity theft crimes. Regrettably, it is the consumer who has the most direct interest in fighting the crime. Indeed, a U.S. Navy commander whose identity was recently stolen told a U.S. House of Representatives panel discussing identity theft on June 25, "Anything you can do to hold accountable those agencies that carelessly extend credit without appropriate protections against fraud, and anything you can do to improve the accountability of the credit reporting agencies, will be significant."

Accordingly, banks and other FSPs must be pressured by consumers and lobbyists to proactively back these efforts:

- **The U.S. Fair Credit Reporting Act:** This piece of federal legislation is being debated by the U.S. Congress and the Bush administration. The act would cover the security and accuracy of personal financial information and access to credit and other financial services. Congress is reportedly going to adjust the system to address consumer priorities, including identity theft and correcting errors in credit histories.
- **BITS' Work on Identity Theft:** The BITS task force on identity theft is working with its member financial institutions to make it easier for victims to report the crime; for example, through the implementation of a single point-of-contact at the financial institution as well as a single victim affidavit. That affidavit concerning the theft could be shared across the consumer's financial institutions so that a different form would not be required for each one. BITS also is trying to institute measures that will help prevent the crime in the first place through education of its members on best-prevention practices and strategies, providing educational materials to customers to help them protect their financial identities, and by working with law enforcement agencies to help analyze and prosecute fraud rings.

Most importantly, however, banks and FSPs must implement solutions that effectively screen for application fraud, so that they don't wrongfully extend credit to identity thieves. A wide range of tools have arisen in the market (see "Identity Theft Fraud Prevention Solutions Start to Proliferate").

Bottom Line: Incidents of identity theft are rising but most criminals get away with the crime, making it a lucrative business for thieves. Banks and other financial service providers typically misclassify the crime, making it easier for the criminals to escape the law. These institutions must receive incentive from legislation and consumer-group pressure to step up prevention efforts that make it harder for the thieves to operate. Without industry prevention efforts, consumers whose identities have been stolen will continue to bear the brunt of social and indirect economic costs — costs that can exact a steep toll for many years.

Acronym Key

BITS	Bankers Roundtable Technology Secretariat
FSP	financial services provider
FTC	U.S. Federal Trade Commission