Javelin Strategy & Research

2007 Trends

In Financial Risk & Fraud

A Javelin Strategy & Research White Paper

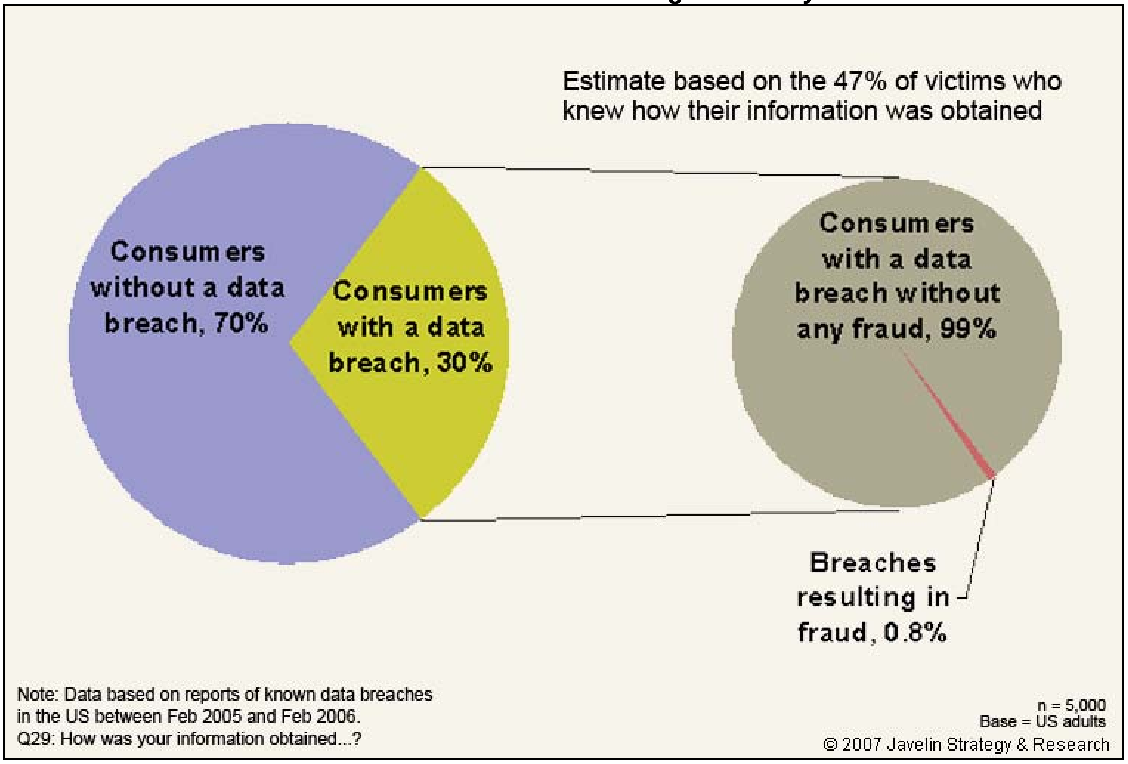
April 2007

About Javelin Strategy & Research

Javelin is the leading provider of independent, industry-specific, quantitative research and strategic direction for payments and financial services initiatives. For more information on this project or other Javelin studies, visit www.javelinstrategy.com

Identity Fraud: Using Facts to Cut Through Speculation

Number of Data Breaches Resulting in Identity Fraud



Identity fraud reality does not match with consumer perceptions. The numbers of US victims of identity fraud and incidence rates have decreased every year from 2003 through 2007[1]. Additionally, the total one year fraud dollar amounts dropped 11.5% from $55.7B to $49.3B over the last year. Mean consumer costs for identity fraud did increase from $431 to $535, or 24%, but the majority of consumers pay nothing out of pocket. Mean resolution hours fell in 2007—lowering the opportunity costs paid by consumers—from 40 hours down to 25 hours (with a median resolution time of 5 hours). Regardless of the decreases in identity fraud, however, 8.4 million victims and $49.3B in dollar losses add up to a very serious source of crime. Currently, 68% of Americans utilize the online channel; and any new channel brings new types of threats. Online hazards are often overblown, as online access only accounted for 16% of identity fraud among the 42% of identity fraud victims who know how their data was stolen.[2] Additionally, data breaches accounted for only 3% of identity fraud among actual victims in 2007. Media hype has played into consumer fears, perpetuating existing misperceptions (especially about the online channel), but has also served a necessary and vital component in educating about the risks of unprotected or improperly protected data. For FIs and networks, correction of misplaced assumptions through further consumer education can allay unnecessary fears and reduce anxiety about exposure to identity fraud. Consistent, well-defined messaging is needed to convey this communication to consumers.

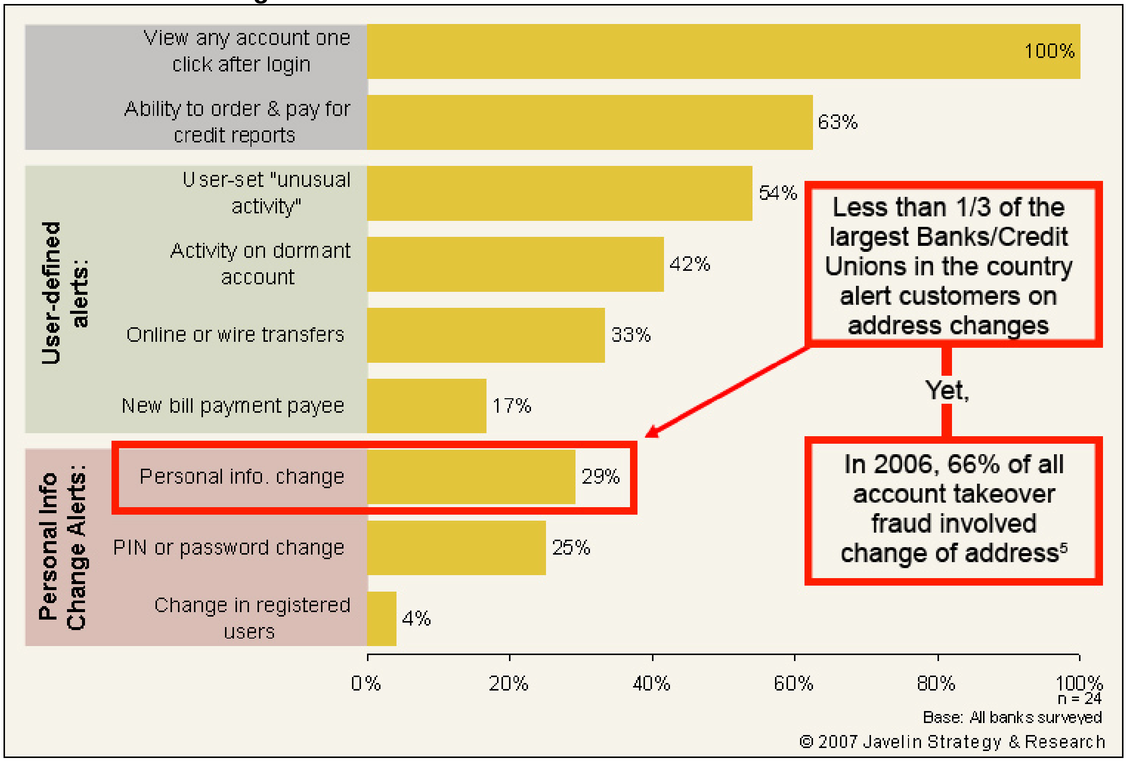
Compared to the attention they receive and the high numbers of consumers receiving notifications, data breaches actually account for only a very small portion of actual identity fraud in the US. In 2006, just 0.8% of data breach victims suffered an identity fraud. It is likely the preventative actions taken in data breaches avert identity fraud in many cases. As discussed, identity fraud remains a prevalent and very serious crime despite the fact that progressive action is being made. To illustrate, one out of every ten consumers has directly experienced identity theft (over lifetime). Eight percent have experienced new account fraud, one of the most difficult types of fraud to detect.

[1] Please refer to **2007 Identity Fraud Survey Report**, Javelin Strategy & Research, January 2007.

[2] Ibid

Enhanced Customer Control Reduces Bank and Merchant Fraud

Banks Offering Javelin's Recommended Customer Fraud Detection Features



Security executives are fighting back against escalating criminal attacks, strengthening authentication, integrating systems and functions across business lines, and meeting various compliance challenges—and as a result identity fraud has declined 12% since 2006.[3] Risk and fraud experts' best work has traditionally been distant from the customer, but criminals' increased ability to successfully impersonate the customer—or the bank or payments firm itself—means that institutions that partner with customers will most successfully foil the common enemy. Javelin's annual Safety Scorecard results show that banks' and issuer's greatest effectiveness lies in after-the-fact victim resolution (the average provider scored 66%), yet experience and federal guidance led to 50% achievement, an improvement, in the prevention category. Technology advancements from UDLAPs to email or mobile alerts allow institutions to deputize the customer™, making for a powerful detection alliance. Customers value this role, with 60% believing that protection of their accounts is a shared responsibility;[4] and, in fact, 47% of all fraud cases are initially identified by the victim.[5] IFMs sent via email or by phone will bolster technology ROI by lowering actual fraud and strengthening loyalty, while also assisting with location-specific marketing offers.

To protect brand and minimize losses banks and issuers must overcome disconnects between current mitigation capabilities, emerging fraud needs and customer desires, as shown in nationally-representative research of fraud patterns and customer preference. Comprehensive research data can also lead to effective product investment roadmaps, providing a gap-analysis tool when multiple information sources are compared. For example, less than one third of FIs offer alerts for personal address changes,[6] yet criminals employ such changes in fully two-thirds of all account takeovers.[5]

[3] **2007 Identity Fraud Report**, Javelin Strategy & Research, January 2007
[4] **Data Breaches & Buyer Behavior**, Javelin Strategy & Research, March 2007
[5] **2007 Identity Fraud Report**, Javelin Strategy & Research, January 2007
[6] **2006 Banking Identity Safety Scorecard**, Javelin Strategy & Research, October 2006

About Javelin Strategy & Research

Javelin is the leading provider of independent, industry-specific, quantitative research and strategic direction for payments and financial services initiatives. Javelin rigorously researches technology issues, industry trends, attitudes and activities of consumers, small businesses, institutions, processors, merchants, billers, and other organizations in order to deliver relevant, high-impact findings. For more information on this project or other Javelin studies, visit www.javelinstrategy.com/research, or send questions/comments to inquiry@javelinstrategy.com.

About this document's featured contributors

Rachel Kim
Within Javelin's *Risk and Fraud* practice, Ms. Kim authors studies to help companies evaluate technology solutions and operational procedures that lead to effective practices in security, brand protection and loss avoidance, using analysis of preference, behavior, and perception data from identity fraud victims, consumer research, executive interviews and mystery shopper research.

Mary Monahan
Ms. Monahan brings 10 years of successful direct financial services industry experience to her clients. Her banking background includes extensive managerial experience working with growth businesses, strategizing and implementing cross-sectional financial plans to accommodate multiple projective scenarios. As a college educator, Ms. Monahan's work focused on current issues in accounting and economics.

James Van Dyke
Javelin's President works on a variety of emerging topics to ensure a match between client needs, rigorous methodologies and action-ready recommendations. With over twenty years in product management or research, Mr. Van Dyke is quoted extensively within the industry and around the globe.

Core Topics

Payments Consumer Confidence
Online Banking, Cards & Billing
Identity Fraud
Forecast & Growth Recommendations
Multi-Channel Cross-Selling
Payment Provider Security
Adoption & Loyalty Factors
Program Adoption Strategies
E-Statements & Payments
Transaction Processing Satisfaction
Peer Benchmarking for Excellence
Competitive Intelligence
Consumer Purchasing Attitudes