White Paper

Stopping Fraud Where It Starts: The Value of Analytics in the Onboarding Process

Ineffective fraud prevention destroys profit margins. The right analytics keeps your business on target.

Syndicated Research
Custom Research
Strategic Consulting

Research provided by Javelin Strategy & Research

February 2010

Risk Solutions
Financial Services

Executive Summary

Difficult economic conditions appear to have reversed the trend of decreasing fraud incidence. According to Javelin's 2009 Identity Fraud Survey Report, the rate of identity fraud rose nearly a full percentage point in 2008. Over the past 12 months, the number of identity fraud victims increased 22 percent to 9.9 million adults. Considering fraudulent new accounts, the data also shows that the gains of 2007 reversed course this past year as the total annual cost of new accounts fraud rose from $15 billion in 2007 to $18 billion in 2008.

It is more crucial than ever to minimize the risk that faceless online applicants are fraudsters. Financial institutions are using a complex, two-phase process that begins by accessing and analyzing a wide range of databases to verify the applicant's identity, then assesses the likelihood that funding for the new account comes from a legitimate source.

Financial institutions must arm themselves with the appropriate tools to combat new account fraud while remaining usable to the consumer. This toolkit ranges from internal initiatives to calling on external experts to review applicant data.

It is designed to assist in defining the good applications from the bad and, where necessary, take further steps for those that fall into that gray area.

Analytic solutions allow financial institutions to create more precise, efficient and automated processes for making smarter decisions. Financial institutions should employ fraud systems that can flag suspect transactions and applications, stop the fraudulent ones and allow the legitimate activity to proceed unhindered. The operational efficiencies gained in addition to the mitigation of risk provide significant benefits to deploy an analytics solution.

Questions answered in this paper

1. What is the current state of fraud, particularly costs and incidence rates?
2. How have new account fraud rates been affected?
3. What is the process for new account onboarding through online channels?
4. Why are analytics so important in an onboarding process?
5. What security tools are currently available to financial institutions?

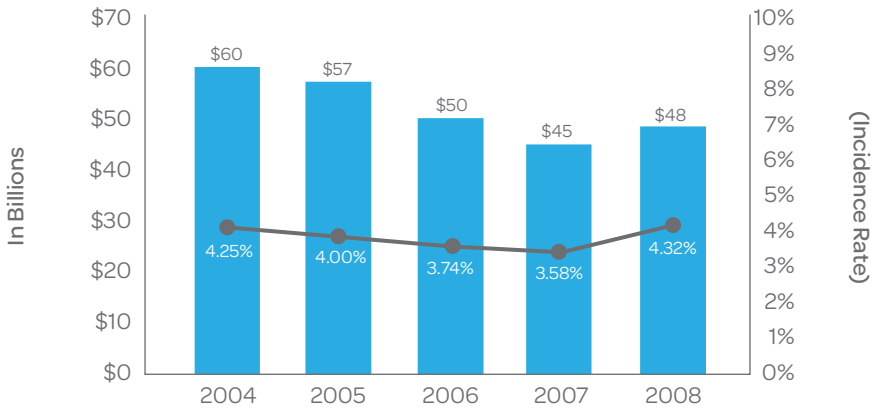
Current state of fraud

Fraud cost and incidence rate

According to Javelin's 2009 Identity Fraud Survey Report, the rate of identity fraud rose nearly a full percentage point in 2008 to 4.32 percent, reversing a four-year trend of decreasing incidence. Over the past 12 months, the number of identity fraud victims increased 22 percent to 9.9 million adults. There have been reports of an increase in crimes of opportunity, seemingly driven by economic misfortune and availability and the deliberate targeting of immediate gains. Simultaneously, fraud increases have been driven by the development of an increasingly global, hierarchal, specialized criminal enterprise and a growing secondary market for stolen financial credentials.

Fraudsters appear to be moving more rapidly, with one notable trend showing a significant increase in data used immediately after the compromise, which jumped from 33 percent to 71 percent over the past three years. There was likewise a rise in data used after a long holding period (one or more years), which grew from 4 percent to 9 percent. This dichotomy speaks to an inclination in which crimes of opportunity are beginning to evolve within a global criminal enterprise that uses the secondary market for large "dumps" of card data, withholds the stolen information and delays its sale to avoid detection.

Total Annual Cost of Fraud and Incidence Rates 2004-2008[1]



Q32: What is the approximate dollar value of what the person obtained while misusing your information?

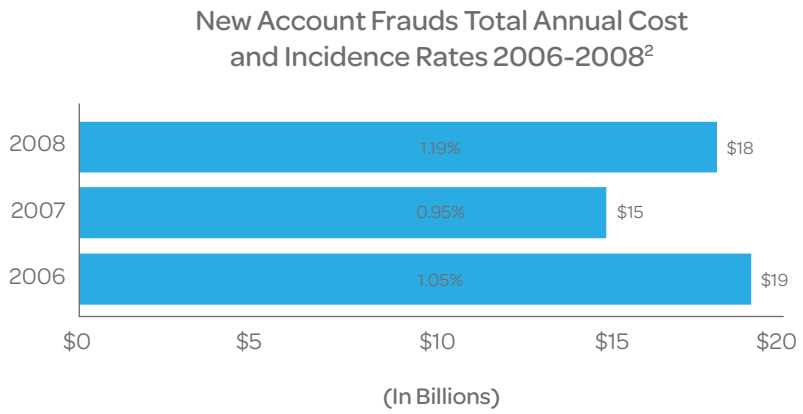
2008;2007;2006;2005;2004, n = 4474;5075;5008;5003;5004
Base: All respondents.

New account fraud

Difficult economic conditions appear to have caused a resurgence in the most frightful form of identity fraud: new accounts establishment. The data shows that the gains of 2007 reversed course this past year as the total annual cost of new accounts fraud, which had decreased from $19 billion to $15 billion in 2007, rose to $18 billion in 2008. The incidence rate of new accounts fraud increased 0.24 percentage points from 0.95 percent in 2007 to 1.19 percent in 2008.

This is a complicated type of fraud to resolve, requiring more than 40 hours of the victim's time to resolve. New accounts fraud is also the most difficult type of identity fraud to detect at 155 days (of the three main categories). These victims are significantly more likely to find out about their frauds by being contacted by a debt collector or by law enforcement (more than three times as often as victims of existing card fraud). Thus, the average duration

of misuse of new accounts fraud is the highest compared to other fraud types at 155 days. New accounts fraud victims tend to have their information misused over a long period of time, i.e. more than one year (20 percent for new accounts versus 9 percent for all fraud victims). They are much less likely than average victims to discover the frauds within the first week and much more likely to discover the frauds after three months or even a year or more. The mean fraud amount for this type of fraud increased 5 percent from $8,386 in 2007 to $8,515 in 2008, while the median amount remained at $3,000.

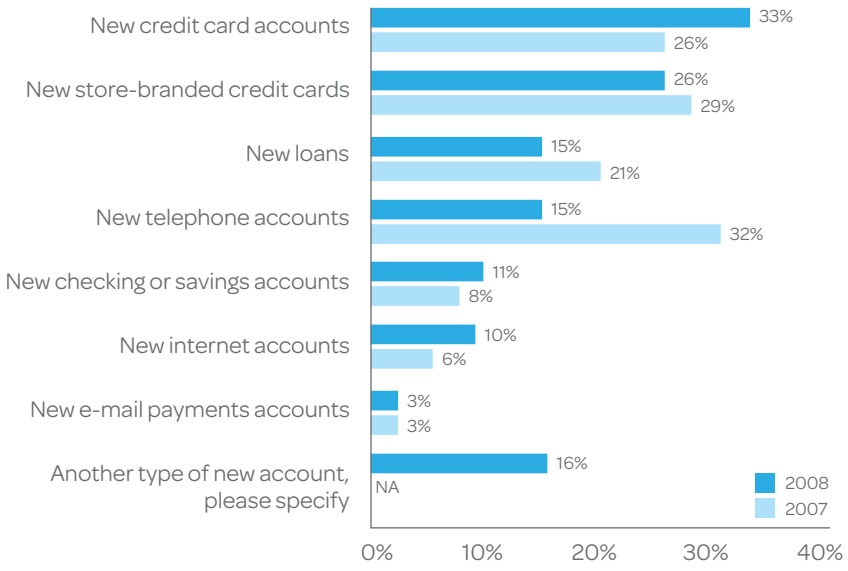


Q32: What is the approximate dollar value of what the person obtained while misusing your information? by Q11: Did the perpetrator use your personal information to obtain NEW credit or debit cards, new bank account or loans in your name, run up debts in your name, open other new accounts or otherwise commit theft, fraud or some other...

October 2008, n = 490/4784,445/5000,458/5000
Base: Card fraud victims.

New accounts victims are likely to be younger: 36 percent of victims ages 18 to 34 experienced new accounts fraud compared to only 19 percent for those 55 and older. Latino victims were also more likely to suffer new accounts frauds (47 percent Latinos versus 32 percent of all victims). New accounts fraud also poses great financial impact to the victim. Four out of every ten new account victims ranked themselves in the more or most severely impacted category (38 percent ranked severe impact versus 25 percent ranked average impact), demonstrating the profound impact of new accounts fraud. Therefore, these victims are the most likely to file a police report.

Types of Fraudulent New Accounts Opened[3]



Q18: Did the person use your information to open any of the following new accounts?

October 2008, n = 146, 137
Base: New account fraud victims.

In 2008, a lower percentage of new account fraud victims reported being defrauded by new store-branded credit cards than did in the previous year (26 percent in 2008 vs. 29 percent in 2007). There were also decreases in the number of victims defrauded by new loans in 2008; 15 percent of new account fraud victims in 2008 as opposed to 21 percent in 2007. These decreases may be partly due to FIs and creditors implementing more sophisticated means of back-end fraud detection capabilities when one applies for a loan or credit card, in addition to being aware of the most recent defrauding schemes and techniques.

Under federal law, banks must abide by the Know Your Customer (KYC) regulations of the USA PATRIOT Act and Bank Secrecy Act (BSA), and are therefore required to perform robust due diligence in customer identity verification.

In 2008, there were a higher percentage of victims being defrauded by new network-branded credit cards (i.e., new cards usable anywhere) than in 2007 (33 percent in 2008 versus 26 percent in 2007). Moreover, an increasing number of victims were defrauded by new checking or savings accounts—up three percentage points from 2007 to 11 percent in 2008. Victims defrauded by new Internet accounts saw an increase from 6 percent in 2007 to 10 percent in 2008.

With identity fraud rates rising for the first time in five years, it is more crucial than ever to minimize the risk that faceless online applicants are fraudsters.

This trend further highlights the need for consumers to take a proactive, rather than reactive, approach to the prevention and detection of identity fraud given the difficulty involved in detecting this type of fraud. The largest decrease was in new telephone accounts, where a 17 percentage-point decrease was observed between 2007 (32 percent) and 2008 (15 percent). The networks have made great strides in this area, especially reducing cloning of accounts.

Current onboarding processes

Account opening is a two-phase process

To the consumer, the process of opening an account online is one that should be simple and proceed without requiring a phone call to the bank or a visit to a branch—a fate suffered by 39 percent of consumers who attempted to open a checking account online in 2008, according to Javelin data.

What the consumer doesn't see is a complex, two-phase process that begins by accessing and analyzing a wide range of databases to verify the applicant's identity, then assesses the likelihood that funding for the new account comes from a legitimate source. With identity fraud rates rising for the first time in five years [4], it is more crucial than ever to minimize the risk that faceless online applicants are fraudsters.

This behind-the-scenes process is often triggered before the consumer completes the application. The first step is to develop a picture of the applicant so a financial institution can determine whether he or she is a customer it wants to do business with. This typically is done by reaching out to third-party data providers like LexisNexis® that sift through mountains of public records, credit bureau files, government databases and other material.

On a basic level, financial institutions will match information listed on the application against routine records to screen out riskier applicants or those identified on federal anti-terrorism lists. But some financial institutions will go deeper, either by consulting a broader number of data sources or by digging deeper into the applicant's history. The goal is to identify applicants who might have a history of fraudulent activity or have been forced to close accounts in the past. Some might run a "soft" credit check that won't show up on the applicant's credit record but will elicit information only a legitimate applicant is likely to know, such as the size of a mortgage payment.

While these steps are mostly motivated by fear of fraud, they also can benefit applicants with thin credit files, such as recent college graduates or the "underbanked." For example, financial institutions might evaluate cell phone bills or driver's license data to develop a better sense of whether the applicant is reliable enough to invite in as a customer. Ideally, data developed during this first phase is evaluated during the application process, resulting in either an approval or a rejection. But many applications will fall into a gray zone, requiring financial institutions to review them manually.

Applicants who make it through this first screening process then face the second phase, when financial institutions must determine whether applicants are making authorized deposits to fund the new account. Many institutions will again rely on third-party data providers to assess the validity of the applicant's claim to the funding account or when booking future accounts.

Some financial institutions are leery of relying solely on this data, in part because it is often weeks old. Instead, they will employ microdeposit authentication that involves making small deposits into the funding account and confirming the amounts with the applicant. Because that process often can take several days—boosting the odds that the applicant will lose interest or forget to follow up—some institutions instead employ account aggregation tools that elicit real-time or near real-time account data. Applicants provide their log-in information to the funding account, and the financial institution confirms information listed on the application. Ideally, the entire process is completed entirely online, in mere minutes.

What tools are available to financial institutions?

The new account toolkit for financial institutions

Rising fraud rates and the wide availability of personal information on the black market means every application comes with the risk of requiring a write-off. Financial institutions must arm themselves with the appropriate tools to combat new account fraud, while remaining usable to the consumer. This toolkit ranges from internal initiatives to calling on external experts to review applicant data. It is designed to assist in defining the good applications from the bad and where necessary, take further steps for those that fall into that gray area.

Customer identification

To comply with KYC (know-your-customer) regulations, applicants are required to provide identifying information that can be checked for validity. Information provided typically includes the applicant's SSN, driver's license or passport number, address and phone number. Institutions additionally run this information against outside data to confirm the information submitted is valid and the identity elements (SSN, physical address or phone number) can be verified. An image of the photo identification (faxed or photocopied in-branch) may be required prior to funding the account.

Device fingerprinting

Device fingerprinting reviews key variables in the device submitting an online application (and the software running on that device) to ensure that it reflects the information contained in the application. Comparing both software and hardware components can ensure, for example, the computer submitting an application claiming to be from Los Angeles, California, is set to Pacific Time or the browser is configured in English and not Russian.

Hot lists

A hot list compiles the relevant data of past frauds and suspicious or high-risk activity. By storing this information for future review and integrating it into monitoring activities, financial institutions can protect themselves from being fooled twice by the same method. For example, by storing the name or IP address used in an application that resulted in a costly fraud, an institution can immediately flag any additional applications with the same information for additional review before authorizing the account. Hot lists can additionally lead to many false positives, as "bad" IP addresses may become "good" IP addresses if a legitimate customer obtains it. Financial institutions must weigh the costs of manually reviewing applicants that hit a hot list due to these false positives.

Outside data

Reviewing outside data during an application is commonplace for identity verification, authentication or fraud scoring. Credit bureau or public record data can be used (beyond the traditional use of spotting for closed-down or delinquent accounts) to fuel KBA (knowledge-based authentication) "out-of-wallet" questions to the applicant.

Financial institutions must arm themselves with the appropriate tools to combat new account fraud while remaining usable to the consumer.

For example, an applicant could be asked the size or institution that holds their car loan or mortgage. Additionally, outside agencies may be called upon to verify that the applicant's data is internally consistent without actually verifying the information. For example, checking whether the SSN on the application matches the year of birth stated by the applicant.

Post-origination monitoring

Monitoring accounts for high-risk transactions or session activity is essential to prevent costly fraud losses. While some institutions forego monitoring for applicants with a prior relationship with the institutions or for accounts older than a window period (be that 60 days, 6 months, 2 years or longer), fraudsters can begin to predict these window periods and create "sleeper accounts" to wait out any window periods before the misuse begins. These "exclusion rules" that determine what transactions or applications are excluded from monitoring must be under review and adapt for changing fraud patterns. If a fraudster gets stopped using a wire transfer at $10,000, they will lower their attempts to $2,000 to slip through monitoring systems.

What makes analytics so important?

Analytic solutions allow financial institutions to create more precise, efficient and automated processes for making smarter decisions. Financial institutions have the responsibility of handling millions of transactions and applications each day. The challenge lies in sifting through those millions of transactions and applications to identify the suspect activity and finally determine which suspect activity is fraudulent.

Impact of incorporating analytics

The key factors in incorporating analytics into your authentication and fraud detection process will be the impact on reducing write-offs due to fraud, reducing manual review while maintaining a smooth process for legitimate activity.

For financial institutions, this has a direct impact on the bottom line by reducing costs and an indirect impact by preventing disgruntled customers from blaming the institution for the misuse conducted in the customers' names and speeding up the process for suspect-but-legitimate activity.

Reduce write-offs due to fraud

Preventing write-offs due to fraud has the most direct ability to reduce overhead. Fraud is a constantly moving target and requires systems that continually adapt to new methods of misuse. Incorporating analytics allows institutions to remain one step ahead of the fraudsters.

Reduce manual review

Manual review of transactions and applicants poses a daunting task for institutions in both time and expense. An analytics solution that screens out obviously fraudulent activity allows analysts to more efficiently process the "gray" transactions that may be legitimate or may be fraudulent. This automation can reduce the average cost sunk into verifying a transaction and allow transactions and activity to be verified faster.

Maintain a smooth process for legitimate transactions and applications

While customers generally appreciate the diligence shown by institutions, a flagged transaction that turns out to be legitimate is inefficient. This draws away from the customer experience and causes undo strain in the banking relationship. Remote channel banking activities are under increasing customer pressure to occur in real time, to keep pace with customers who want their bank to move as fast as they do. Employing analytics can get new accounts started on the right foot for these customers.

Recommendation

Financial institutions

The data shows that the gains of 2007 reversed course this past year. The incidence of identity fraud increased by 22 percent in 2008, with fraud amounts increasing slightly from $3 billion over the previous year. Difficult economic conditions also appear to have caused a resurgence in the most feared form of identity fraud: new accounts establishment. It is more crucial than ever to minimize the risk that faceless online applicants are fraudsters.

Financial institutions are tasked with sifting through millions of transactions and applications each day. Without the proper technology in place, that process is a daunting task that requires excessive work hours to manually review these transactions.

Financial institutions should employ fraud systems that can flag suspect transactions and applications, stop the fraudulent ones and allow the legitimate activity to proceed unhindered. The operational efficiencies gained in addition to the mitigation of risk will reduce write-offs due to fraud, reduce manual review of suspect activity and maintain a smooth process for legitimate transactions and applications. Financial institutions will see this direct impact on the bottom line in reduced overhead, more productive analysts and fewer customer complaints.

Sources

[1] 2009 Identity Fraud Survey Report: Identity Fraud on the Rise but Consumer Costs Plummet as Protections Increase.

[2] Ibid

[3] Ibid

[4] Ibid

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.