Fraud detection in newly opened accounts

Connecting data helps predict identity theft

Experian℠

Fraud detection in newly opened accounts

Executive summary

Fraud continues to be a genuine threat and challenge. After a sharp and unexplained drop in identity thefts in 2010, fraud schemes climbed 12.6 percent in 2011, according to research by Javelin Strategy & Research. The cost adds up: The mean cost for new-account fraud is $3,197.[1] If someone succeeds in opening up an account, it typically has taken a mean of 151 days to detect the fraud occurrence.[2] As a result, fraudsters have become savvier and more opportunistic. Increasingly, they're likely to attack the institutions with the weakest defense. At the same time, old tactics to identify fraud may be insufficient. Fortunately, the latest technologies and a new Experian® weapon — Precise ID℠ for Customer Management — offer the opportunities to improve fraud detection substantially, especially very early in the Customer Life Cycle. Precise ID for Customer Management incorporates relevant and timely data to help improve decision making — data that may have been unavailable during the early life of accounts. This paper explores how this new service helps detect identity theft and other fraud, how data velocity can prove the key to predicting identity theft, and still deliver a strong and quick return on investment.

The identity theft challenge

An estimated 11.6 million American adults, or nearly one in 20, were victims of identity theft last year. The price tag? An estimated $18 billion. Fraudsters also are becoming more patient. They may open a few accounts to make sure the compromised identity can be used to obtain credit or services. Once this information is confirmed, the fraud perpetrators will open numerous accounts in one to 15 days.

Like a contagion, identity thieves are growing savvier and more opportunistic in getting what they're after. Increasingly, crooks are mastering ways to steal someone's personal information via social media or mobile devices as well as traditional routes, and they're often preying on the institutions with the weakest defenses. Credit card fraud schemes, for example, involving identity theft climbed 12.6 percent in 2011 after dropping sharply the previous year.[3]

Simply consider the massive fraud that 30-year-old, Nigerian-born Canadian Adekunle Adetiloye managed to oversee and pull off. He opened up 600 fake bank accounts at 22 banks and piled up $5 million in fraudulent charges before he was apprehended. In January, he was sentenced to more than 17 years in a U.S. prison for masterminding the plot.

How he did it underscores just how shrewd and resourceful fraud artists are becoming. Among other things, he incorporated two debt-collection companies. Through them, he gained access to commercial-data providers that only exchange information with other debt-collection firms, financial institutions and law-enforcement agencies. That access let him retrieve private and sensitive information on tens of thousands of people. Posing as the real customer, he opened credit card and other accounts and used these new credit lines to rack up fraudulent charges.

[1] 2011 Javelin Strategy & Research 2012 Identity Fraud Report, February 2012, page 35
[2] Ibid., page 21
[3] Ibid., page 6

Fraud detection in newly opened accounts

Adetiloye's flagrant mischief explains the need for a fraud account-management system to continue to detect fraud for new accounts in particular. If one statistic tells the story, it's that a fraudulent new account costs on average $3,197.[4] Old tactics simply may be insufficient today to uncover criminal activity like that perpetrated by Adetiloye.

In addition, some lenders simply contend, "We have the strongest defense against identity theft at origination. Why should we check again after the accounts are opened?" Further, every lender to some degree allows a certain amount of fraud to get through because the cost of ferreting out all of it would prove prohibitive. Fraud review rates vary from customer to customer.

If lenders require any more evidence that they must be increasingly vigilant, they need only to consider the increase in the number of consumers notified that their data had been lost through one of the many data breaches that took place in 2011, and the potential accounts that could be opened. According to Javelin Strategy & Research, data breaches increased last year and statistics showed that 19 percent of data breach notification recipients experienced fraud.[5]

Data to the rescue

Fortunately, advances in data access and analysis have delivered new weapons to flag suspicious consumer data patterns early in an account's history. In addition, a lender's ability to use the latest tech artillery, which consider more relevant and timely data, leads to improved decision making — and an answer to the question, "Why should we check again?"

Today's principal new tool, Precise ID for Customer Management, takes advantage of data previously unavailable or aggregated after an initial application and authentication transaction, to identify and prevent current-account fraud during the early life of an account being opened. This gives lenders additional insight into fraud riskiness during the early life of accounts. Accounts that may have appeared lower risk when opened may have actually been, or turned, high-risk because of activity picked up by the Precise ID for Customer Management service — holistic link analysis that determines how data (more than 2 million new records per day) is used across numerous identity-related transactions across multiple industries and businesses.

A lender also might want to check its new-accounts portfolio again just to ensure that an identity fraudster didn't choose it among his or her first few victims. During the application process, it's often difficult to detect fraud because the potentially limited view of data available at that point of authentication may appear to be consistent and sound.

[4] *Ibid., Figure 11, page. 21*

[5] *2011 Javelin Strategy & Research 2012 Identity Fraud Report, February 2012, page 39*

Precise ID for Customer Management establishes intricate identity linkages across Experian's broad expanse of consumer transactional data. Experian is able to access activity across the entire country and can tap into data assets other individual institutions cannot. The analytical fraud-detection tool is risk-based and creates scores and examines attributes, finely segmented pieces of information correlated with consumer behavior that can expose potentially fraudulent activity readily within existing portfolios.

Using Experian's vast network of transactions, Precise ID for Customer Management evaluates these attributes to reveal threats of identity theft as well as fraud activity being perpetrated during or post application that can be linked to inconsistent or high-risk use of numerous identity elements.

For instance, this tool lets a credit issuer lower the risk of high identity fraud among recently booked and even more established existing accounts. It can point Experian's vast resources toward those accounts warranting additional authentication and monitoring.

Precise ID for Customer Management allows clients to segment risky accounts. It also lets reviewers alter decision thresholds and account treatments over time and evaluate identity risks associated with questionable accounts and customers at any point in time. Scores are available on demand or processed in batches. This allows reviewers to categorize and rank order any number of accounts quickly and cost-effectively.

Pinpointing questionable behavior

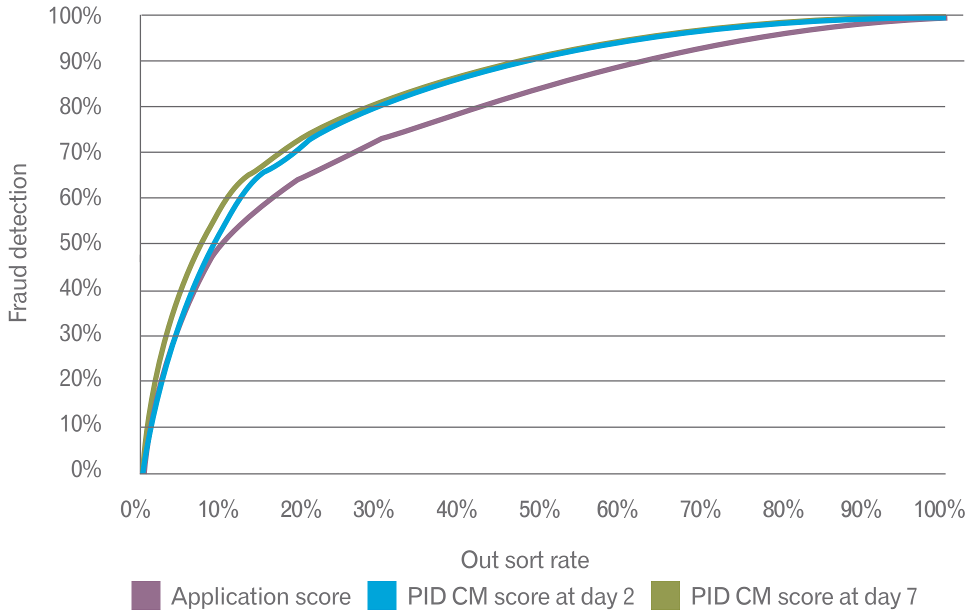
Here's how a customer can pinpoint questionable behavior with Precise ID for Customer Management. When an account opens, a customer can employ the tool initially to examine elements tied to the consumer. Many are familiar, such as name, address, Social Security number, phone number and other specific identity information. It prepares a base score at that time, usually on Day 0 of the new account. Then, on the seventh day, the customer initiates another inquiry to determine what has changed. Perhaps the data shows that a credit customer is using a new phone number while keeping other information the same when applying for new credit or services.

If a reviewer notices a large degree of inquiry activity tied to a consumer's identity or identify elements, it suggests that fraudulent activity may be occurring, and the reviewer can tag that account for greater scrutiny. The tool is looking for inconsistent use of data elements over time. For example, if the phone number used at Day 0 shows no inquiries tied to it but now shows seventeen new inquiries linked to it at Day 7, this could indicate fraudulent behavior.

Fraud detection in newly opened accounts

Precise ID for Customer Management validation result

Precise ID^{SM} for Customer Management score from day 0 to 7



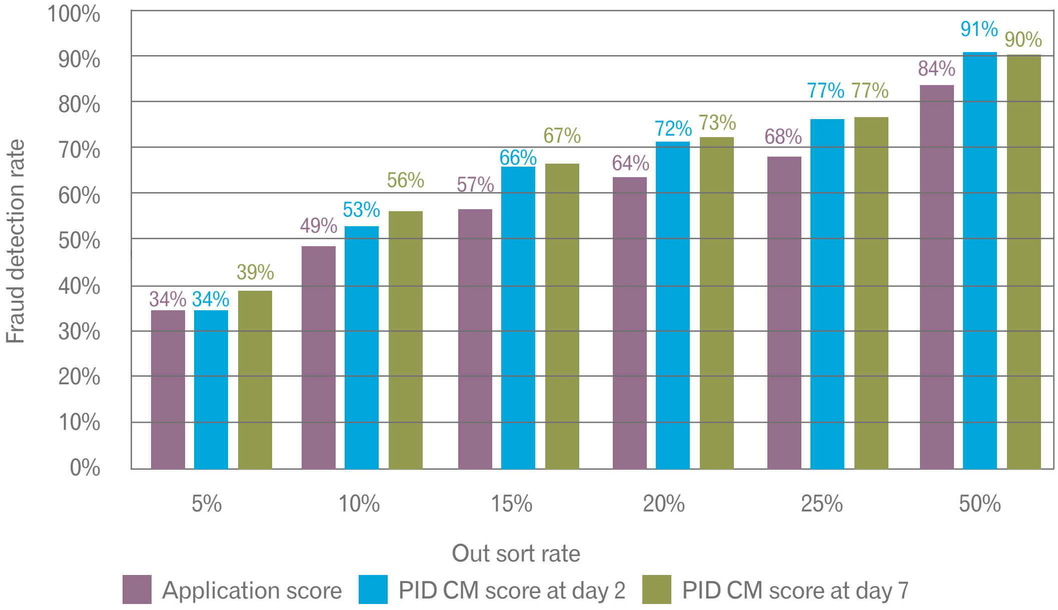
Within the lowest scoring 20% of the population, an increase of 5% to 10% fraud captures can be achieved within the first seven days post application.

Experian has found that at Day 7, the Precise ID for Customer Management score can find an additional 7 percent of the fraud occurring when reviewing 10 percent of a lender’s portfolio and an additional 10 percent of the fraud at a 15 percent review rate. This fraud percentage is incremental over using typical front-end fraud scores.

Fraud detection in newly opened accounts

Precise ID for Customer Management validation result

Precise ID^{SM} for Customer Management time lapse comparison from day 0 to day 7



Time lapse comparison shows up to 10% fraud capture gains after 7 days post application using the Precise ID^{SM} for Customer Management score.

Fraud “lift” can even be found on Day 0 in many situations, and this results in the ability to find an additional 5 percent of identity fraud. Precise ID for Customer Management also delivers a good lift of questionable activity when the account is examined after it is 15 days old, but results fall off during the 15- to 30-day period.

The savings generated by uncovering such fraud is substantial, because the mean cost for new-account fraud in 2011 was $3,197, according to Javelin Survey & Research’s 2012 survey of identity fraud.

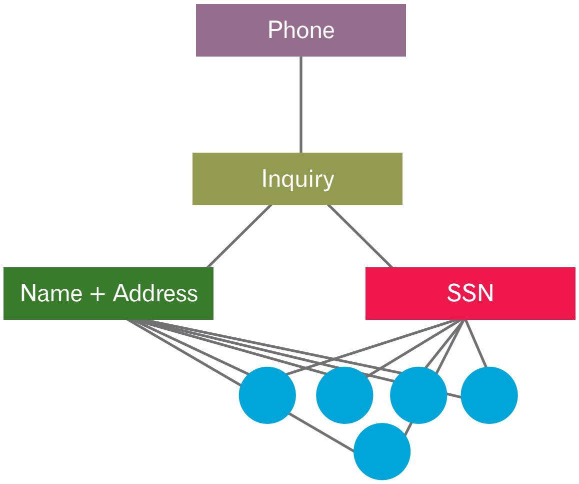
This indicates that fraud artists move swiftly within the first two weeks, perhaps assuming they can stay undetected that long before credit companies can begin spotting the suspicious activity. This also would explain why such questionable incidents drop in the second half of the first month in which an account is opened.

The technology also can focus on increased activity — the speed at which a fraud artist acts to open account after account with stolen identity information. For instance, at some early point, it can detect if someone has applied for multiple types of accounts, such as a retail card account or a new cell phone. The data is cross-industry, so fraud perpetrators can’t hide behind the use of data if they aren’t using credit data.

Fraud detection in newly opened accounts

New account fraud example — Day 0

This graph and the subsequent graphs will demonstrate how the cluster of records that are attached to this fraud record build over time for this fraud case.



- Phone, name + address and SSN keys are extracted for this inquiry record
- Number of historical transaction records that match any of these keys is determined
- In this example, 5 historic transaction records match on name + address and SSN
- Features based on these linkages that are used for scoring the inquiry record
- Notice that no historical transaction records are linked to phone

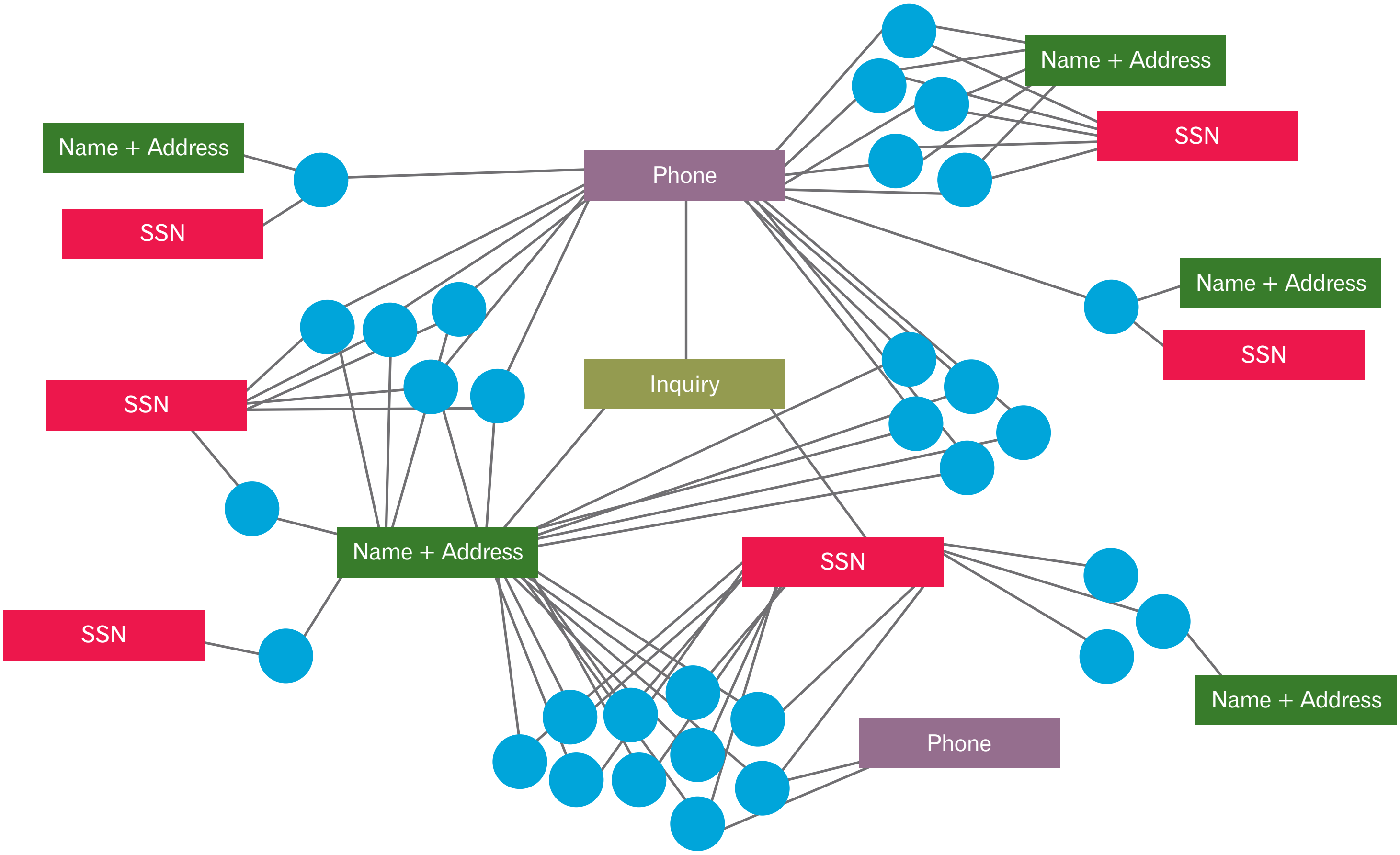
● Historic transaction record

The Precise ID for Customer Management score snares suspicious activity triggered by changes in behavior — activity that might be missed otherwise. For instance, if someone applies for credit soon after doing so elsewhere, the Precise ID for Customer Management score can point out any major differences in how the data was used across the various applications for credit or services.

Fraud detection in newly opened accounts

New account fraud example — Day 7

This is the same inquiry record as in the previous slide except we have now moved forward 7 days. Notice all the additional connections that have occurred.



● Historic transaction record

For example, if the date of birth was omitted but the same name and Social Security Number were given, that could set off an alarm. If an applicant gave a different phone number but the other information was the same, another alert could be sounded. By comparing a person's pattern of behavior — in terms of what elements they present when applying for products and services — the technology can signal instances when these behavior patterns change.

Conclusion

The 2012 report on data breaches and identity theft from the respected Javelin Strategy & Research firm underscores the need for more advanced tools to help credit companies, banks and others detect and nab fraud perpetrators, who steal billions of dollars from them and innocent consumers.

Last year, victims of a data breach were 9.5 times more likely to be a victim of identity fraud. Consumers who received a data breach notification had a fraud incidence rate of 19 percent, while consumers who didn't receive such a notification had a rate of 2 percent. Also, with a shocking 67 percent jump in data breach victims in 2011, the increase correlates directly with the rise in identity fraud victims.

This rise in identity crime comes as banks and other credit-granting organizations continue to look for ways to improve their profit margins on their credit holdings.

Experian is leading the way in identifying and developing new tools to help institutions corral both new-account and existing account fraud. With its vast repository of data from a growing roster of sources, Experian is best able to develop a highly predictive service such as Precise ID for Customer Management.

475 Anton Blvd.
Costa Mesa, CA 92626
www.experian.com

Experian℠
A world of insight

04/12 • **5527/5111** • 6228G-CS