experian®

Precise ID℠

An integrated approach to the world of identity risk management

White paper

Abstract

Identity risk management has emerged as a discipline designed to tackle losses in a grey area of overlap between credit and fraud management. This grey area is independent of how credit and fraud losses may be classified by individual institutions. This paper explores the emergence of identity risk and its first-party and third-party identity fraud components. The paper considers the necessary elements of an identity risk management strategy and details the requirements that any solution needs to provide to be marketable. Finally, it introduces Precise ID,℠ a new solution offered by Experian which seeks to provide the most comprehensive identity risk management solution on the market today.

Background

Patterns of fraud are constantly evolving

The pattern of financial fraud is constantly evolving. Criminals exploit weaknesses in fraud defenses and, in turn, institutions block these gaps through the introduction of new policies and/or technologies to prevent further losses. Additionally, changes in the marketplace lead to new products and services, which inherently bring with them new risks to be exploited and the cycle repeats itself.

Fraud trends that have emerged most recently include:

1. **Increase in the velocity of fraud:** Knowing transactions are monitored for suspicious patterns, the fraudster understands that a compromised card has a limited time utility. Fifty to 75 percent of fraud losses can occur within 24 hours of a card being compromised and the loss can frequently be a result of the first few transactions. Trying to contact the customer after the transaction(s) has occurred does little to prevent the loss.

2. **Internationalization of fraud:** Specialized criminal gangs increasingly work outside of the United States to gain access to account information. They then perpetrate crimes online which is driving a rapid increase in card-not-present fraud. They can also exploit under-the-floor limit transactions or areas where authorization networks are traditionally weak.

3. **Payment fraud:** As the choice of electronic payment methods increases and controls to prevent check fraud improve, fraudsters, sensing vulnerabilities, are looking to Automated Clearing House (ACH) and balance transfers as alternative methods to stealing funds.

4. **"Phishing:"** The theft of personal information, e.g., PIN numbers or account numbers, by using phony institution Websites or through sending e-mails requesting such information. Losses from PIN debit cards are rising as a result, albeit at negligible levels.

Card issuers have progressively improved in spite of challenges

Despite these trends, fraud losses, as reported by card issuers and expressed as a ratio of fraud losses to sales, have decreased by more than 50 percent in the past 10 years. Most U.S.-based card companies report net fraud losses in a sustainable four to 10 basis point range. Overall, U.S. credit card fraud losses amounted to an estimated total of $1.32B in 2004[1].

The downward movement on these loss rates has been achieved through substantial investments in fraud detection and prevention technologies, e.g., neural networks, card activation, real-time authorization decisioning. These have served to cut losses from traditional fraud scams such as mail theft and counterfeiting.

Despite these investments and noted success in stemming losses, public concerns over financial fraud appear to be higher than ever. The Internet channel suffers significantly higher loss rates than other conventional channels (CyberSource estimated 1.8 percent of sales are lost to fraud)[2]. There are also sustained concerns around the

[1] Financial Insights, 2004.
[2] CyberSource, 5th Online Fraud Report, 2005, p. 4.

Recent examples of highly publicized cases include:

1. In March 2005, Designer Shoe Warehouse disclosed that personal credit card and banking information for 1.4 million customers had been stolen from its database.
2. In June 2005, CardSystems Solutions, Inc., disclosed that a breach of its system to process transactions between merchants and credit card issuers exposed 40 million accounts to possible fraud.
3. In March 2004, BJ's Wholesale Club reported that the cards of approximately three million customers may have been compromised as a result of the theft of data from its credit card database.

potential for identity theft losses as a result of stolen personal information. A number of highly publicized and ongoing cases of data compromises serve to heighten consumer sensitivity around identity theft.

In addition to these cases, there is ongoing regulatory pressure from the government to ensure adequate authentication of customers, in order to prevent money laundering and financing of terrorist activities. This requires financial institutions to continue to upgrade and invest in new fraud defenses. Financial institutions that fall behind the innovation curve run the risk of significant exposure to highly unpredictable losses. This risk not only occurs in the form of immediate increases in financial losses, but also in lost business revenues due to declining consumer confidence.

Defining fraud: Emergence of identity risk

Definitions of fraud are not always clear-cut

While card associations have attempted to categorize fraud into traditional fraud types, e.g., lost/stolen, counterfeit, nonreceived, etc., such classification is increasingly fraught with difficulties and may actually be detrimental in the development of loss reduction strategies. Some of the factors which drive the issues surrounding classification include:

1. **Multiple fraud types within one case:** Many fraud cases involve several fraud types, e.g., counterfeit fraud can involve card-not-present transactions.
2. **Customer fraud:** The customer claims fraud even though they legitimately made the transactions. Despite best efforts to investigate these types of cases, ultimately some cases are charged off as fraud.
3. **Agent/Institution discretion:** Individual institution policies and training with regard to fraud vary considerably. This provides wide discretion on when and how losses are defined.

The lines between first- and third-party fraud are often blurred

Nowhere is this classification problem more apparent than in recent attempts to quantify the losses generated by third-party identity fraud and in the growing awareness of first-party fraud. In theory, the difference between the two is clearly definable:

1. **Third-party**, or **identity theft**, is the criminal use of another person's identifying information, e.g., name, address, Social Security number, date of birth, etc. Using some or all of these as his own, the identity thief may apply for a credit account or gain access to the victim's savings, checking or other accounts. Third-party theft also includes **account takeovers**, when someone changes an account name or address to gain control of the account. These losses are typically recorded as *fraud* losses.
2. **First-party fraud** occurs when an individual applies for credit using his or her actual identity, but with no intention of paying. This includes **early payment defaults**, when little or no payments are made after

getting a loan or other type of credit, and **bust-outs**, the sudden and complete use of credit limits on an account or accounts with no intent to pay. These losses are typically recorded as *credit* losses.

In reality, there can be overlap between credit and fraud losses (Figure 1). It is in this area of overlap where the role of a unified management approach to identity risk is beginning to evolve.

For example, in a case of **synthetic identity fraud** in which identities are fabricated and no victim steps forward to claim fraud, accounts are charged-off as a credit loss before the institution is aware of the problem. In faceless application processing environments,

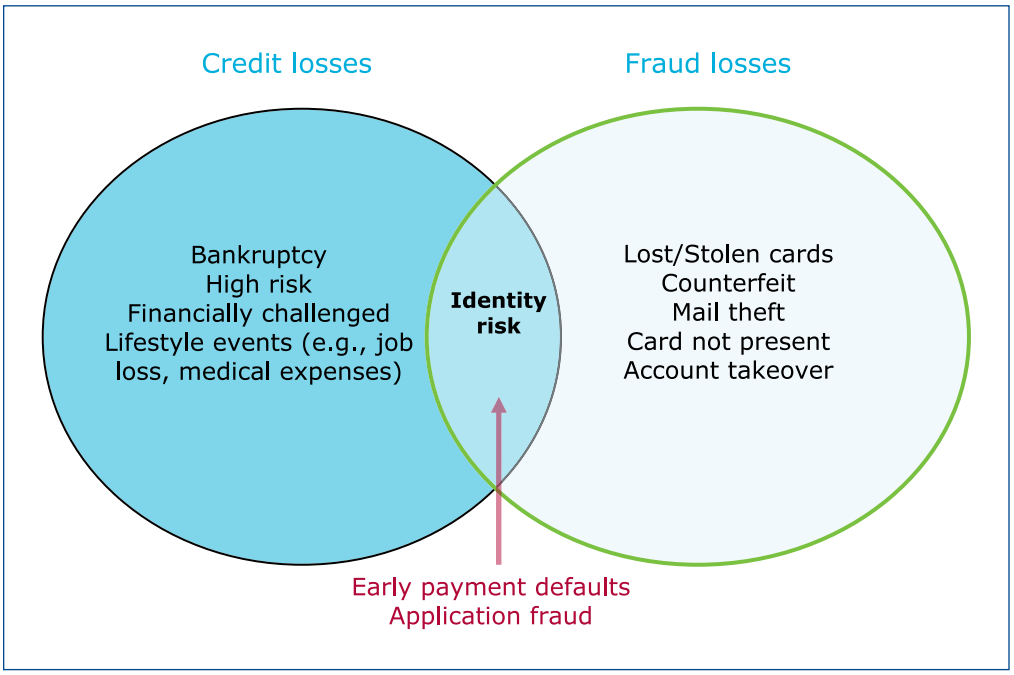


Figure 1: Overlapping worlds of credit and fraud losses

the difference between third-party stolen information with intent to defraud or first-party manipulation of their own personal information with intent not to pay can be very difficult to discern without detailed analytics.

True estimates of the extent of identity fraud losses are hard to determine and actually vary by degrees of magnitude depending on the methodology and/or definitions used.[3] In 2005, the UK government estimated the loss to the economy from identity fraud to be £1.3B affecting some 120,000 individuals.[4]

It is likely, however, that even in a well-run operation some identity fraud is recorded as a credit loss. Financial Insights has estimated that more than 70 percent of identity fraud goes undetected as fraud and is eventually reported as credit loss.[5]

First-party fraud losses are even higher than third-party fraud losses

Perhaps more significantly, many fraud managers indicate that first-party fraud losses can account for 80 to 100 basis points of loss, dwarfing the losses of third-party identity fraud. They are also concerned about the rate of growth. In the United Kingdom, for example, reports of first-party fraud cases are up more than 90 percent in the four years since 2000.[6]

[3] From a low of $6B (Financial Insights, 2005,), to a high of $56.6B Javelin Strategy & Research, January 2006, "2006 Identity Fraud Survey Report."

[4] *The Guardian* "ID Theft is a growing Concern for UK Consumers," Jan. 9, 2006.

[5] Financial Insights: "Fraud Management Technology: Evolving with the Times," 2004, p.3.

[6] CIFAS Press Release, April 28, 2005.

This is due in part to a proliferation of programs that target sub-prime markets that, in general, have thinner or nonexistent credit records.

Managers increasingly realize that similar solutions can be used to tackle both third-party and first-party fraud losses. Hence, the emergence of identity risk management; a discipline which puts individual loss recognition policies aside and focuses on the development of a unified solution to the problem. Furthermore, these managers understand that solutions are best deployed during the application process using the latest predictive modeling techniques and data from a variety of sources.

Market demand for identity risk management

Classic credit models are able to generally rank order the risk of a customer defaulting on outstanding loans. Account management and collections tools can then be used to manage credit loss within a certain range of risk tolerance. However, these models are limited in their ability to detect fraud, including first-party fraud. By the time these accounts default and reach the collections stream, it is too late to avoid a credit loss. The ability to model this first-party fraud activity remains a significant challenge for individual credit grantors.

Credit managers have typically been faced with a classic dilemma with regard to preventing application fraud: Approving applications with the future risk of an undefined and unpredictable future loss, or manually reviewing large numbers of suspect applications to prevent losses. This results in costs paid both in terms of higher operating expenses (false positives), and lost revenue from legitimate consumers who are denied credit (false negatives).

The negative file approach

Historically, financial institutions relied on a set of individual "hits and flags" and negative files to alert them to potential suspicious application activity, e.g., address, Social Security number mismatch. Individually, these alerts created a significant amount of false positives, e.g., due to keying errors, and allowed fraud to occur undetected. Over time, these alerts were combined and more complex rules were written which marginally improved detection. More sophisticated solutions were created using logistic regression models. However, they lacked the benefits of consortium data (from multiple cross-vertical creditors) and relied upon batch data which quickly aged, thus affecting performance.

Today's solutions use "risk-based" approaches and sophisticated analytics

Today, companies are increasingly turning to external business partners with access to multiple data sources in order to deploy innovative analytical techniques to spot anomalies. These business partners are able to detect suspicious activity using a broader perspective, rather than that seen by just one company or within an industry vertical. They also have fresher data available from which to base their analytics.

Institutions demand higher fraud detection rates while seeking to minimize their costs. They also need these solutions to balance the economic trade-offs inherent in the process by allowing them to make optimized decisions. These decisions need to be based on sound analytics. Solutions must accomplish this while strictly complying with the regulatory environment in which they operate.

What the market is demanding from identity risk solutions

Experian, based on conversations with its customers, has identified several key factors influencing market demand for identity risk solutions. Solutions must:

1. **Comply with the regulatory environment** — Solutions must comply with the relevant sections of legislation (federal Fair Credit Reporting Act, USA PATRIOT Act, Gramm-Leach-Bliley Act, etc.).
2. **Easy to integrate** — Solutions must be "easy" to integrate with existing legacy application processing systems.

3. **Provide flexibility** — Solutions must recognize the changing patterns of fraud and the different channels used to acquire accounts.

4. **Highly predictive** — Models must rank-order risk better than other solutions, i.e., detect more fraud while impacting fewer good customers. They also need to be able to identify both first- and third-party fraud patterns.

5. **Customizable** — Recognizing that each customer is different, solutions need to allow for customized rules and the ability to rapidly test and deploy new strategies.

6. **Deliver above-hurdle-rate return on investment** — Solutions must provide a robust return on investment. The set-up and on-going costs must provide a commensurate benefit and payback within an acceptable time period.

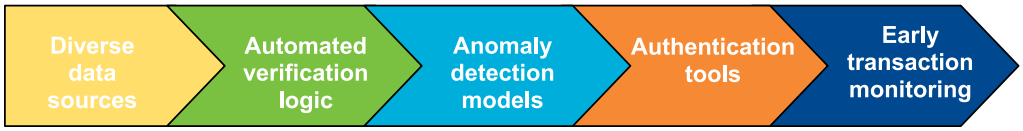


Figure 2: Components of an identity risk management strategy

Developing identity risk solutions

A well-thought-out identity risk strategy should be based on five key components, as outlined in Figure 2 below:

- **Diverse data sources:** Access to large and diverse data sources, including an up-to-date source of validated frauds from which to profile. Access to other application data is critical, but not available to individual institutions.

- **Automated verification logic:** An automated process must be established to match each element of submitted application data with separate validation data sources. There must also be a mechanism to ensure data is internally consistent with the other submitted pieces of data, e.g., does data match that submitted for other applications from the same person. The logic must also include steps to check against Office of Foreign Assets Control (OFAC) lists and meet USA PATRIOT Act requirements.

- **Anomaly detection:** Since mismatched data elements alone are not predictive enough to identify fraud risk, these mismatches must serve as inputs for models. Models recognize suspicious patterns by combining the submitted application data elements and comparing them with irregularities associated with known fraud patterns. The model output takes the form of a risk score. Reason codes should augment the score to assist in the investigative process.

- **Authentication tools:** Once the risk of an account has been calculated, a process needs to be established to cost-effectively and accurately review suspect applications. Tools need to be available for agents to investigate applications in a systematic fashion.

- **Early transaction monitoring:** Approved applications having passed verification but with higher risk scores must be monitored within early life account queues and authorizations subject to specific rules in order to detect risky transactions.

Today's fraud solutions

Most fraud solutions on the market today fall into the following groups:

1. **Single-source consumer authentication:** Based on single source of truth, e.g., a credit report. Using a "challenge-response" method, customers are asked more obscure questions regarding their finances that are unlikely to be available in a victim's wallet, e.g., student loan details.

2. **Multiple-source data validation:** Use of databases to cross-reference information supplied on applications, e.g., driver's license records, Social Security number records.

3. **Suspicious pattern recognition across industries:** Based on a belief that "patterns of the thief's 'footprints' show up across industries much more readily than they do within one enterprise." Using consortium applications and fraud data, companies identify suspicious patterns and alert institutions to the risk level of new applications.

Few products on the market provide end-to-end solutions which cover all elements of a comprehensive identity risk strategy; even fewer provide it at a reasonable cost. For example, many companies produce application fraud risk scores, some of which can be highly predictive, but scores alone do not help in the authentication process once the risk is known. Conversely, there are several "source of truth" data sources to assist in the verification process, but they do not help determine which priority applications should be contacted based on risk.

Precise ID℠ product features

Experian has been developing application fraud models using consortium data for more than 10 years. Based on understanding the needs of the market and the *critical* components of an identity risk strategy, Experian has introduced a new state-of-the-art solution — **Precise ID.**℠ The platform has been designed to deliver a single point of integration and to provide industry-leading performance. Tangible benefits include the ability to detect more fraud, improve operational efficiency and to perform the authentication necessary to meet and surpass regulatory standards. The platform is flexible enough to pull data from different sources depending on the specifications and to run standard or custom-built models.

Figure 3, next page, presents a graphical illustration of the **Precise ID** platform showing the data inputs, process and outputs.

Prospective customers will be particularly interested in the following features:

- **Extensive data sources** — Capitalizes on Experian's position as a leading credit data aggregator.[7]
- **Superior analytics** — As well as detecting traditional third-party application fraud, the models look to flag possible first-payment defaults which may be the result of potential first-party fraud.
- **Flexible decisioning technology** — Allows users to define and customize rules parameters.
- **Authentication questions** — Provides users with recommended next steps including the questions to assist with further verification.
- **Ease of deployment** — Uses an open architecture solution for quick implementation regardless of operating environment.

Precise ID utilizes extensive data sources

Experian is able to draw upon one of the world's largest sources of credit and proprietary noncredit data for use in authentication and the basis for model development. Records include:

- A consumer credit database with more than 215 million credit-active U.S. consumers.
- 200 million cross-industry application records to help detect inconsistencies in incoming applications.
- A national consumer demographic database with more than 400 data sources on 215 million consumers.

[7] Precise ID offers solutions using credit and noncredit data. The GLB-compliant product for identity screening uses internal and third-party databases that do not require a credit-permissible purpose to verify information. It is useful for companies with a high prevalence of faceless transactions but no permissible purpose to view credit reports, e.g., consumer-oriented Web sites or retailers. The FCRA-certified product for account opening uses credit data and is ideal for financial institutions. The tool posts a "soft" inquiry to the person's credit file, making the inquiry available for view only to the person applying for credit and the initial inquiring institution. That avoids potential impact to a credit score due to excessive inquiries.

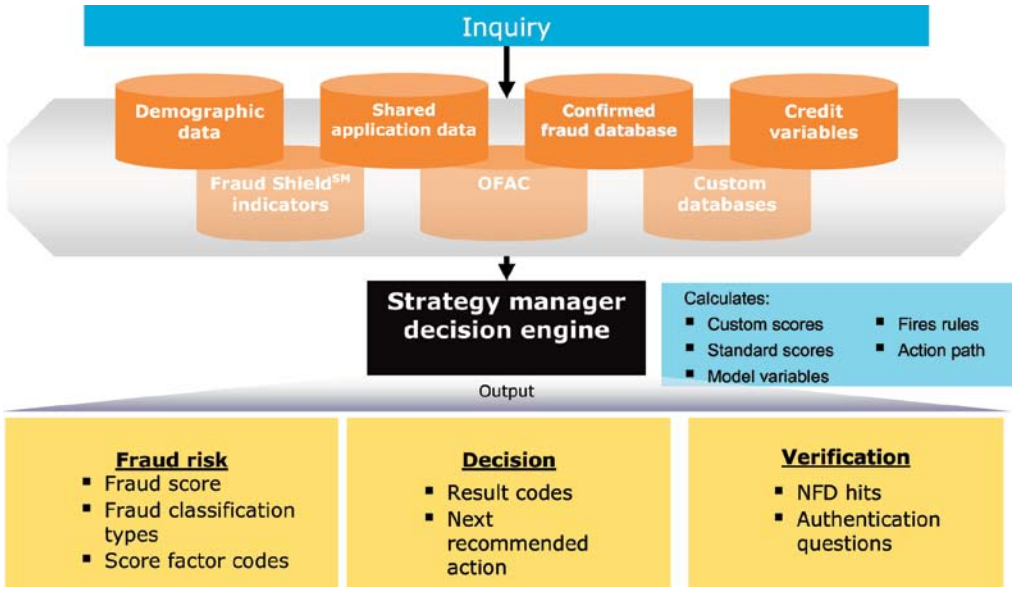


Figure 3: Precise ID platform

- An automotive registration database with more than 150 million records.
- A property ownership database with more than 83 million records.

In addition to these records, Experian has the world's largest record of verified frauds contained within its pre-existing National Fraud Database.℠ Containing more than 400,000 fraud records from banks, credit card issuers, telecommunications providers, and retailers, this database is invaluable for use in identifying fraud patterns. Precise ID also accepts custom data elements upon inquiry.

Superior analytics

With sophisticated modeling techniques Precise ID produces an identity risk score that accurately assesses levels of first-party and third-party fraud risk. The Precise ID score is driven by logic which scores applications for the accuracy of data supplied (validation) and for the probability that this data is true (verification). Applications that need further review are prioritized according to the level and type of risk to help achieve the most cost-effective screening process. Separate verification and validation scores can be returned in addition to the overall identity score to assist in determining the appropriate investigative procedures to follow.

In an industry first, Precise ID models distinguish fraud types to achieve a single, actionable fraud classification, characterizing possible first payment default, identity thefts, fraud rings and synthetic identities which support enhanced authentication strategies. The fraud classification codes are based on the premise that different fraud types exhibit markedly different profiles. Modeling the individual elements of each profile significantly enhances model performance and classification.

As a direct result of superior model performance, users who typically experience double-digit referral rates can expect a significant reduction in referral volumes with no degradation in fraud detection rates, or conversely reduced fraud losses with maintained referral levels. Alternatively, clients can work with Experian's consulting staff to optimize these trade-offs according to the specific economics of their business model, e.g., accepting a slightly higher rate of fraud in exchange for higher revenues from applications that might otherwise have been declined.

Flexible decision technology

The Precise ID platform incorporates a leading decision engine technology. By leveraging the strategy manager decision engine, users have considerably more flexibility than many rigid systems to change rules in response to changing

patterns of fraud. Or if they choose, clients can customize strategies so that they can apply their unique knowledge of their own customers and specific fraud patterns to the problem of authentication.

The platform houses all the standard models, calculates derived variables and allows for multiple process flows. The platform also has the flexibility to house custom models, as well as the capability to allow for champion-challenger strategies. The platform also has the ability to seamlessly export all of this data, models and results of the strategies back to the client's decision/application processing system.

Experian's experienced consultants can assist in customizing strategies for the client's environment while being consistent with industry-best practices. For example, writing rules which vary the degree of verification required, according to the level of loss that may be incurred, assists in minimizing both cost and customer impact.

Authentication questions are drawn from a rich set of data sources, including automobile and public record information, as well as credit accounts and demographics. Precise ID provides user help in real-time, issuing suggested questions and next steps to aid in the authentication process.

Since Precise ID is a hosted solution, it allows for quick implementation in any operating environment, while still maintaining the level of customization that a client may require.

Case studies

A top retail card issuer

Retail instant credit

Retail merchants in general receive the majority of applications at the point of sale, generating instant credit for their customers. Their business models are highly sensitive to fraud controls that generate high volumes of referrals. This often presents a challenge since the fraud rate (frequency of fraud attempts), is often much higher in an instant credit environment than traditional "take-one" or direct-mail campaigns. Finding the optimal balance between fraud control and sales requires a precise approach: Identifying only the most suspicious applications for further review.

The challenge — Lower fraud losses while reducing cost through automation

One large retail client tasked Experian with developing an automated tool for detecting fraud at the point of sale.

The solution — A custom model on the Precise ID platform

After conducting a needs assessment to understand the unique requirements of the retailer's sales environment, Experian performed an analysis of the retailer's accounts and developed a custom model residing on the Precise ID platform.

The results soundly exceeded expectations

The fraud detection rate was 20.5 percent at only a 2 percent referral rate level. By reviewing only 5 percent of the total volume, the client was able to capture a full 46 percent of the fraud.

A large wireless carrier

Wireless service providers

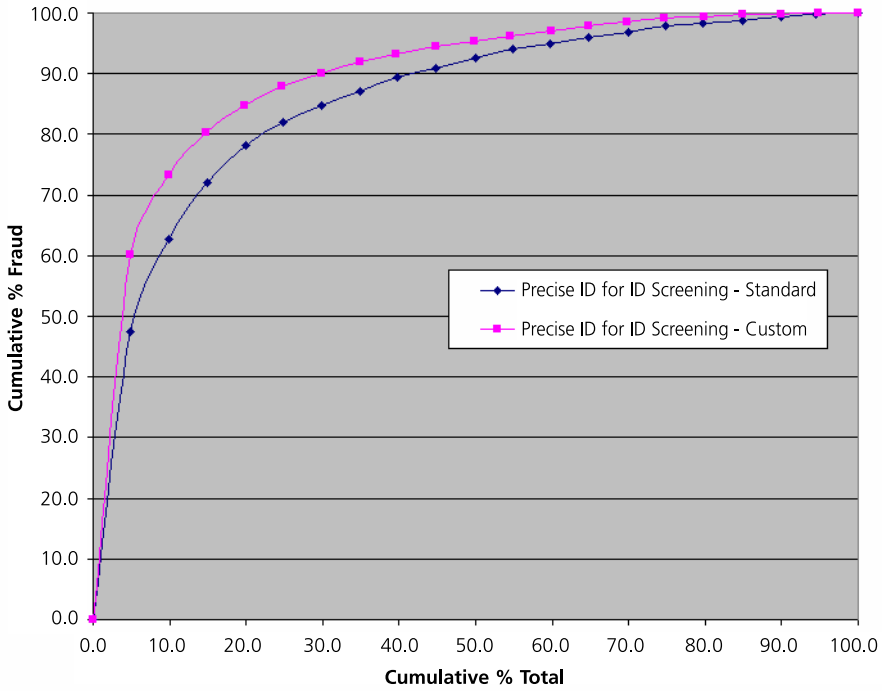
Wireless carriers operate in an extremely competitive environment with switching costs lower than ever before. Approval decisions must be made quickly, frequently online and with minimal customer inconvenience in order to maintain the service levels expected in the marketplace.

The challenge — Lower fraud losses while reducing false positives

One large wireless provider challenged Experian to lower the false positives and leverage superior data sources to shorten the application process while detecting more fraud.

The solution — A custom Precise ID model for identity screening

Experian took a sample of all new service applicants over a three-month period and appended a suite of Precise ID data, variables and scores. From this sample, Experian produced a custom model for identity screening.



The results were impressive

Experian's custom model outperformed the Precise ID standard model by 22 percent. With only a 5 percent review rate, the client was able to capture 60 percent of total ID fraud, up from 47 percent using the standard model, and false-positive rates improved substantially. Experian's custom solution lowered response and cycle times, ensuring top-quality customer service.

An online retailer

Online issuers

Like all online merchants, online credit grantors are exposed to significantly higher risk of fraud than in the offline world. Criminals are drawn to these credit issuers because of the higher potential gain per transaction. At the same time, competition in the online arena is fierce. As a result, retailers must have excellent response times and low false positives to increase sales. Online fraud managers are held accountable for the percentage of time potential customers do not complete sales due to their fraud validation screens.

The challenge — Decrease fraud losses while reducing false positives

One online issuer asked Experian to increase its identity fraud detection rates while lowering review volumes. The issuer saw value in Experian data, but wanted it integrated into one easy-to-use model. The client's current fraud model was capturing 44 percent of the fraud at a referral level of 10 percent.

The solution — A custom Precise ID model for account opening

A sample of 530,000 approved accounts and associated data was used to develop a custom model. The result was a custom Precise ID model specifically for account opening, with a score that rank-ordered risk. Experian took a sample of all new service applicants over a three-month period and appended a suite of Precise ID data, variables and scores. From this sample, Experian produced a custom Precise ID model to assist in the account-opening process.

The results showed a decided lift

Experian's custom model outperformed the Precise ID standard model by more than 52 percent. At a 10 percent refer rate, the fraud detection rate increased from 44 percent using the generic model to 67 percent using the custom model. At only a 5 percent review rate, 52 percent of the fraud was being detected with the new model.

experian®

475 Anton Blvd.
Costa Mesa, CA 92626
800 509 5604