A FAIR ISAAC WHITE PAPER

Innovative Services Need Innovative Fraud Detection

What financial institutions need now to secure new channels and markets for rapid, profitable growth

Scott Zoldi

January 2008

Summary:

As financial institutions expand their markets and deliver innovative services, risk rises as quickly as opportunity. Criminals are quick to exploit any and all vulnerabilities created by new processes, under-protected channels and changing customer behavior. This white paper describes three Fair Isaac analytic techniques—Global Profiles, Self-Calibrating Models and Adaptive Models—that elevate the state of the art in fraud detection to meet the challenge of today's dynamic business environments. Financial institutions can layer these powerful, flexible new capabilities onto their existing fraud detection solutions to further limit risk exposure and improve profitability across both existing lines of business and new initiatives.

FOR MORE INFORMATION

phone from US **1 800 999 2955**

worldwide **1 612 758 5200**

email **info@fairisaac.com**

web **www.fairisaac.com**

Table of Contents

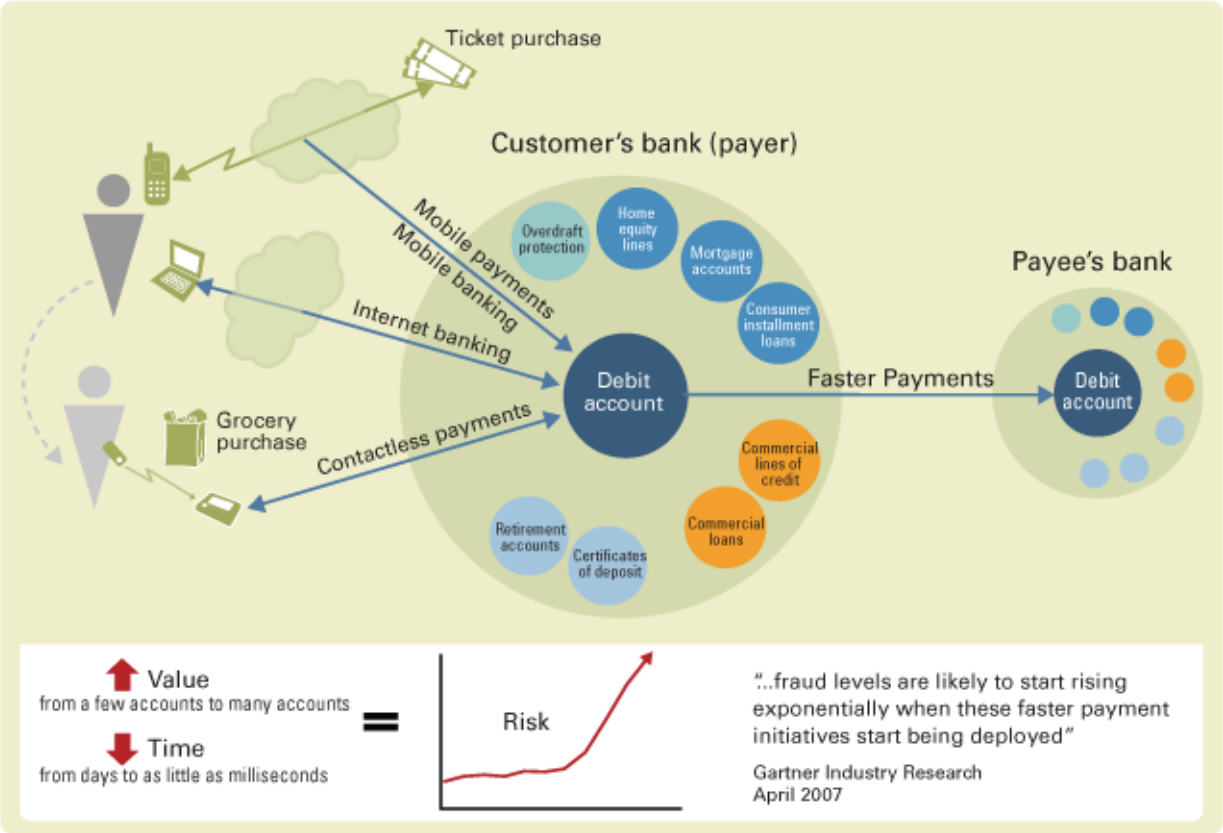
Better fraud detection will help deliver profitable new business

Financial institutions can win big today by providing faster, more convenient payment methods and other innovative financial services. Markets around the world are stirring with new players and delivery channels as technological advances, social change and evolving consumer financial attitudes and practices create significant opportunities.

Financial institutions can also lose big unless they improve their fraud detection efforts to meet the challenges posed by these market conditions. Widespread use of debit cards in place of cash, the increasing trend for financial institutions to position debit accounts as a gateway for additional financial services, growth in online banking, accelerated settlement initiatives like Faster Payments in the UK and the Single Euro Payments Area (SEPA), and the emergence of mobile banking and mobile payments all create irresistibly lucrative and potentially vulnerable targets for criminals.

Offering such services exposes financial institutions to the risk of very large losses in very short time periods. Moreover, a few well-publicized fraud incidents could have a significant impact on organizational reputations, customer confidence and the speed with which new services become adopted and profitable. On the upside, however, financial institutions that meet these new challenges may be positioned to reap greater profits and market share from new services and channels. They'll be able to safely and efficiently approve more transactions, gaining a competitive advantage from higher revenues with lower fraud losses and operating costs.

FIGURE 1: AS OPPORTUNITIES INCREASE, SO DOES RISK



Recent research by Fidelity Information Services shows that in the UK, which has begun the transition to Faster Payments, many financial institutions are recognizing the need to take new fraud detection measures.[1] Quite a few, however, still rely solely on policy rules and rudimentary analytics to catch fraudulent payments in the account to account payment channel. These measures are typically employed over the several days traditionally required for settlement processes. With the settlement window now narrowing, most financial institutions see the necessity of moving phone and online banking, as well as other lines of business involving electronic transfer of funds, onto the real-time transactional analytics that they've long used to detect payment card fraud.

> "Banks can learn considerable lessons from their own card payment operations, in which applications to spot fraudulent transactions in real time have been commonly used for years. These solutions must be expanded to ensure that they cover electronic payments initiated via Internet banking and telephone."
>
> *Faster Payments, Stronger Authentication*
> Gartner Group Industry Research, April 2007

> "For too long, banks have relied on older systems and processes that are not equipped to deal with increasingly sophisticated fraud attacks. [Our] research shows that the thinking has started to change."
>
> Mark Davey, managing director, Europe, Middle East and Africa
> Fidelity Information Services, Nov 2007

But even the current state-of-the-art in real-time transactional fraud detection techniques will not be enough to counter the rising fraud threat in these new offerings. Today's financial markets and methods will require these systems to acquire additional capabilities in three key areas:

- **Encompass the full extent and complexity of financial transactions.** Fraud detection systems must go beyond recognizing changes in customer behavior patterns to recognizing changes in the behavior of, and interactions among, the wide range of other entities (debit accounts, ATMs, merchants, POS terminals, countries, mobile payment kiosks, etc.) playing a role in new market environments.
- **Operate in environments where historical data is inadequate or nonexistent.** In new channels, such as Faster Payments and mobile payments, there is limited historical data or none may exist. Yet these channels must be secured from the onset. In other cases, data from past transactions may exist but may not be useful for building traditional supervised models because they have not been dispositioned (past transactions have not been tagged as fraudulent and nonfraudulent). Or dispositioned historical data may be available to build a model, but it is not fully reliable—for example, when a model developed with data from one country/market is deployed in another country/market. In all these less-than-ideal situations, systems must nevertheless be able to detect fraud accurately.
- **Maintain accuracy amid changing conditions.** The ability to detect fraud in environments that are changing is essential. In the past year, for example, cross-border fraud has risen rapidly in Germany and Italy, and ATM fraud in the US has surged.[2] More gradual climbs have occurred in card-not-present (CNP) and identity-theft-related fraud over the past several years. All of these are instances of evolving fraud patterns and dynamics, which can affect the detection accuracy of models built from historical data. We can expect such dynamic conditions to intensify, particularly in emerging markets. New financial services and channels—and even the implementation of anti-fraud measures—in one market are likely to cause abrupt shifts in fraud patterns within that market, geographically adjacent markets or even markets on other continents, given the increasingly global and mobile nature of fraud. Systems must be able to dynamically adapt to such changes in order to maintain (or even improve on) their original levels of precision.

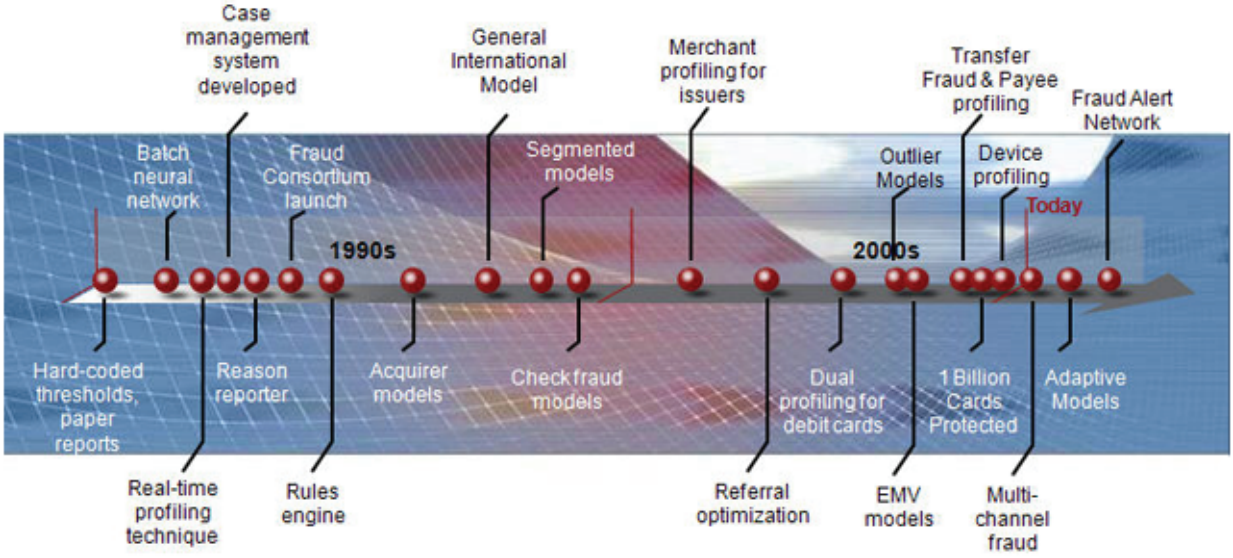
[1] "Fresh Research Shows UK Banks are Changing Their Strategy in the Fight Against Fraud," press release, Fidelity Information Services, 11/29/07
[2] "EMV—The Main Tool in Fighting Card Fraud," Frost & Sullivan, 12/7/07

The good news is that the state-of-the-art in fraud detection has stepped up to the challenge of meeting today's elevated fraud threat. Fair Isaac, the #1 provider of fraud management solutions in the world (Gartner BSS Market Share 2007) has delivered the latest in a two-decade-long series of innovations. Recent advanced technologies that raise the bar in fraud detection include Global Profiles, Self-Calibrating Models and Adaptive Models.

These innovative analytic techniques are today supported by equally innovative software, which provides the processing capabilities necessary for today's demanding business environments. Using some of the same mathematical techniques employed in rocket science, our systems now perform this advanced fraud detection with blindingly fast transaction processing times. End-to-end throughput is less than 200 milliseconds. One client is processing over 1.5 billion transactions in production, day in and day out.

New capabilities combined with existing Fair Isaac fraud detection solutions provide a more powerful and flexible toolkit for fighting fraud in diverse, changing markets. These additional analytic innovations may be employed individually or in combination to create different types of detection solutions for a wide variety of fraud problems.

FIGURE 2: NONSTOP INNOVATION IN FRAUD ANALYTICS



Global Profiles—improving visibility into fraudulent activity

Global Profiles enable fraud detection systems to encompass the full extent and complexity of financial transactions. They provide models with the ability to examine financial processes from multiple views, revealing fraud that is not visible when analyzing customer behavior alone.

Dynamic profiling is the proprietary Fair Isaac technology that enables our neural network models to accurately detect abnormal cardholder behavior in a fraction of a second. Profiles mathematically compress immense amounts of historical behavioral data into carefully selected and highly predictive variables that allow for extremely efficient real-time transactional analytics.

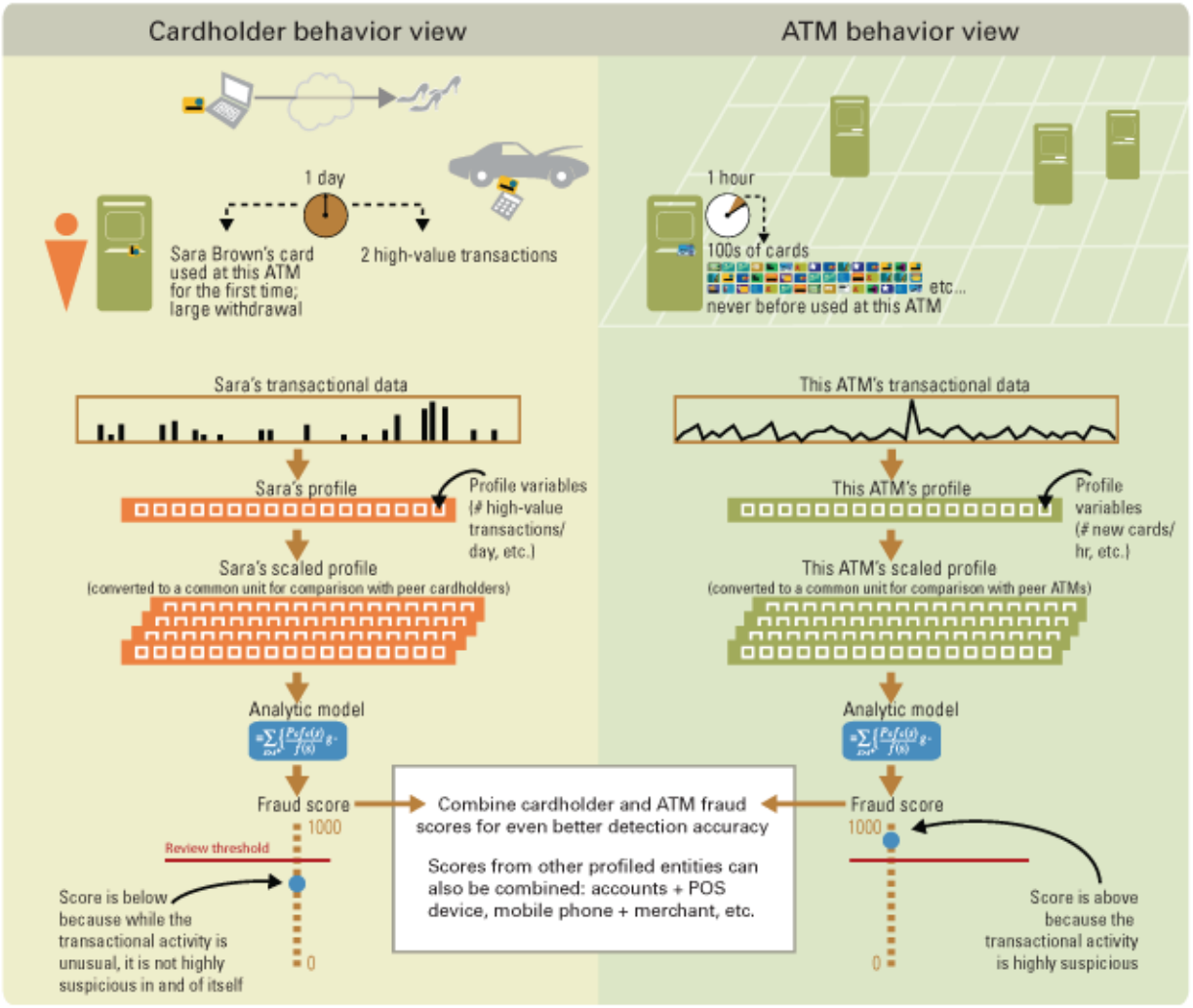
Global Profiles, supported by the software advance of shared memory profiles, expand the dynamic profiling capability considerably. Fair Isaac systems can now not only detect abnormal behavior in cardholders, but simultaneously in other entities as well and in the interactions between them. These additional entities might be other process participants, such as merchants and wireless carriers. They might be geographical units, such

as countries or states. They might be infrastructure or end-user devices, including ATMs, POS terminals, contactless payment devices, mobile phones and telecom switches.

This type of profiling is “global” in the sense that a profiled entity may pertain to more than one customer. A particular ATM, for example, may be pertinent to understanding the behavior of tens of thousands of individual customers. It will also contribute to a “global” picture of what is going on in the financial system and can therefore be used to detect fraud in multiple ways. An ATM profile helps detect fraud at the ATM; in addition, based on aggregate cardholder behavior at that ATM, it improves fraud detection at the cardholder level.

Here’s an example. Imagine a situation where a criminal uses a stack of counterfeit debit cards to steal funds from an ATM. As depicted in Figure 3, if the fraud management system is profiling only customer behavior, it probably won’t detect fraud associated with the ATM device. Sara Brown may never have used that particular ATM before, but that event, while unusual, is not necessarily suspicious. What is suspicious is that several hundred cards have been used at this ATM in the past hour—none of which has ever been used there before. The fraud management system will detect this suspicious activity at the device level only if it is profiling both debit cardholders and ATMs.

FIGURE 3: GLOBAL PROFILES EXPAND FRAUD VISIBILITY TO IMPROVE DETECTION ACCURACY



Similarly, a ring of fraudsters testing the viability of stolen or counterfeit cards by making modest purchases from an online retailer is likely to slip under the radar, at least for a time, of a detection system profiling customer behavior alone. What is suspicious is not that David Murphy's credit card is being used to buy sneakers from an Internet merchant, but that the merchant has experienced 20 times its normal volume in sneaker purchases in the past hour or that the declined card volume has increased by 50 times the normal volume during this period.

Interactions between profiled entities can be revealing as well. For example, a fraud management system with global profiling capabilities might detect an abnormal concentration of card-present purchases by customers in Vermont from merchants in Iowa—and know that this is more suspicious than if the merchants were in neighboring New Hampshire. Consider a similar scenario in a Faster Payments environment, where inter-bank transfers will be completed in as little as 15 seconds. In a fraction of a second, global profiling could focus fraud detection in on an abnormal pattern of first time fund transfers for accounts associated with a bank in Birmingham to a single newly established account in Dover.

Global profiling is extremely flexible, allowing Fair Isaac to work with clients to profile the entities most important to their particular transactional environment. Companies can also take a preventive approach, monitoring transactions with certain entities, such as zip codes that have experienced high concentrations of fraud in the past.

Self-Calibrating Models—detecting abnormal behavior in new environments

Self-Calibrating Models figure out for themselves what normal and abnormal behavior is by analyzing ongoing transactional activity. This enables them to detect fraud even in environments where historical data is missing or inadequate. It also enables them to adjust to changing environments.

As with any of the pooled or custom models that Fair Isaac builds for clients, the first step in the development of self-calibrating models is the application of domain expertise and understanding of the specific fraud problem to determine highly predictive variables. The difference comes at the next step, where standard, "supervised" models are typically trained by analyzing many months of historical transactional data to recognize which variable values are normal and abnormal. Self-calibrating "unsupervised" models are instead put directly into production, where they infer these values of normal and abnormal activity from the transactions they are processing by dynamically scaling variable values (converting them to a common unit for comparison across peer groups) using anomaly detection and other statistical techniques.

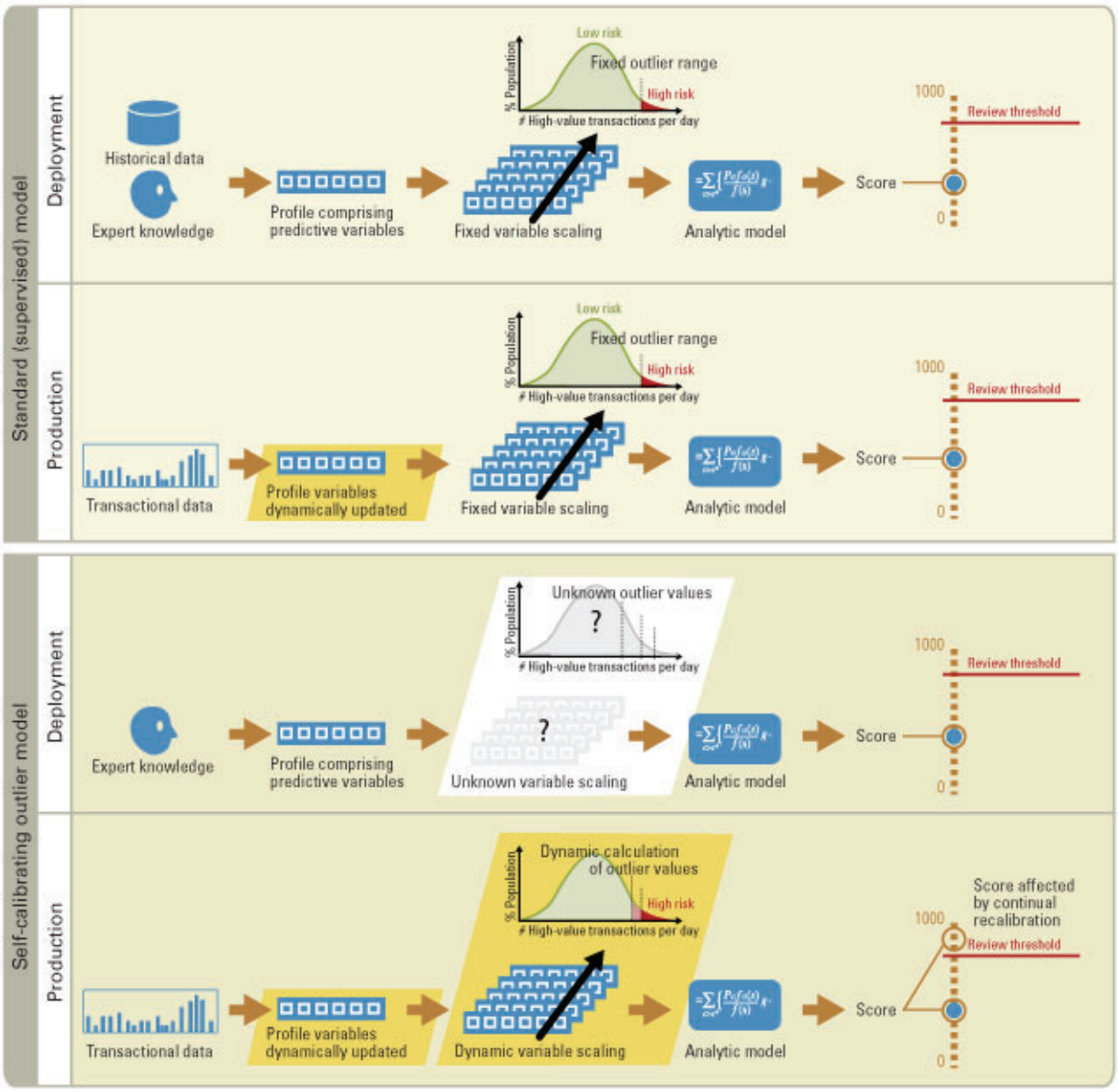
Use in environments where historical data is nonexistent

Financial institutions deploying new services such as Faster Payments don't have the luxury of collecting many months worth of transactional data for building standard fraud detection models. Self-Calibrating Models enable them to begin detecting fraud virtually from launch by identifying outlier behavior on the fly.

For example, as shown in Figure 4, a Self-Calibrating Model performing dynamic variable scaling might determine that for the variable *number of high-value transactions per day*, a value of 3 standard deviations from the mean of the peer group is enough of an outlier to be suspicious. The fraud detection system would therefore use this value in addition to other outlier variables to generate a score indicating high probability of fraud.

A customer's peers might be defined as the bank's entire portfolio of debit cardholders or only those debit cardholders with account balances above a certain threshold. In fact, self-calibrating models can perform outlier analysis within specific segments assigned by the bank, allowing for refinement of the scoring. For instance, pre-assigned peer group segmentation could enable the fraud management system to differentiate between variable values that are abnormal for ATMs at bank branches but normal for ATMs at convenience store locations, or normal for consumer electronics e-tailers but abnormal for brick-and-mortar jewelry stores.

FIGURE 4: FINDING OUTLIERS IN REAL TIME

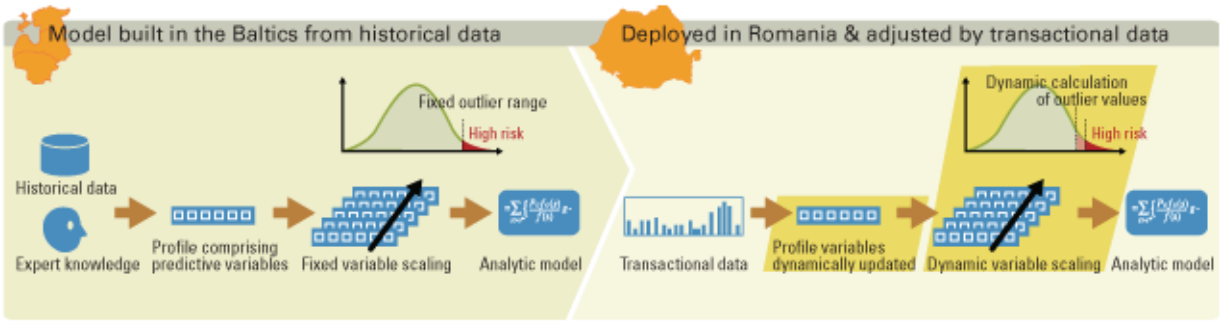


Use in environments where historical data is unreliable

In many situations it is worthwhile to deploy a model even if the data on which it was trained is not a perfect fit for the production environment. In Eastern Europe, for example, there is considerable variation between the maturity of markets for payment cards, bank loans and other financial services.

A standard supervised model developed from historical data pooled from financial institutions in the Baltics, where payment card penetration is relatively high, might be applied to nascent card markets in Romania or Bulgaria. Self-Calibrating techniques would enable the model to rapidly adjust its variable scaling to the different behavior in each country where it was deployed. At the same time, redeployments of the model would benefit from the learning that had already taken place in the Baltics on how to combine the scaled variables.

FIGURE 5: ADJUSTING TO A NEW MARKET



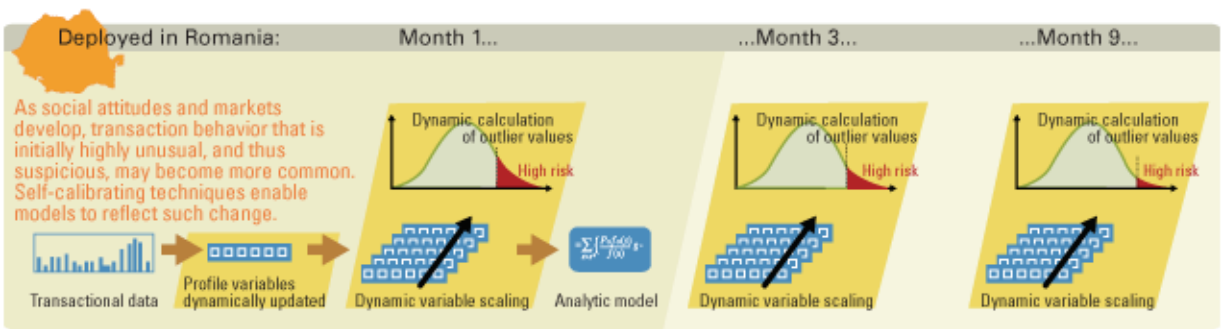
Use in changing environments

Self-Calibrating Models can also be used in conjunction with standard supervised models built on fully reliable data, helping to improve detection accuracy between standard model updates.

In Central and Eastern Europe, for example, rapid social change and new attitudes toward credit make card markets extremely dynamic. Variable values that are outliers today may be normal tomorrow. Dynamic scaling will automatically adjust these values based on ongoing transactional activity.

In the UK, the implementation of Faster Payments may abruptly or gradually change the behaviors of consumers and commercial customers in established payment channels such as debit and credit cards. In Europe, the advent of SEPA is expected to affect not only payments within participating eurozone countries, but adjoining countries as well. Self-Calibrating Models can be layered onto the current fraud detection models in use by financial institutions within affected areas to help them dynamically adjust the variable scaling until the next scheduled model retraining.

FIGURE 6: CONTINUALLY UPDATING IN A CHANGING MARKET



Adaptive Models—accelerating the learning cycle

Adaptive Models immediately absorb the outcomes of fraud case dispositions and apply them to subsequent fraud detection. This enables them to not only adapt to changing patterns of normal behavior, but to quickly recognize the changing tactics of fraudsters.

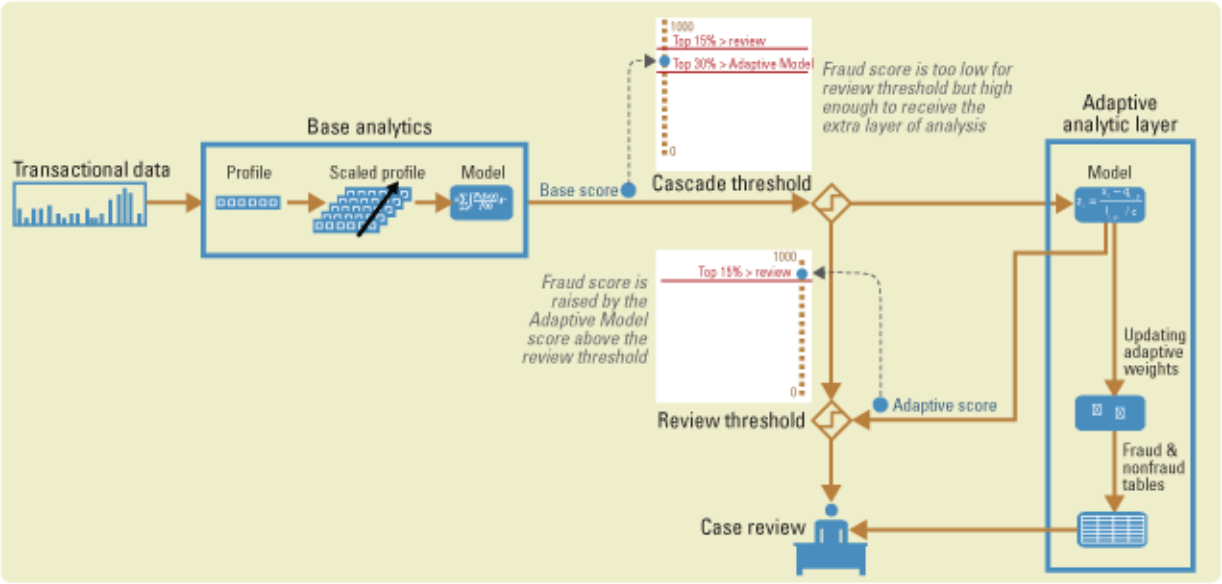
Clients of Fair Isaac utilizing Falcon® Fraud Manager benefit from the combined power of advanced analytics and the industry's best business rules management system (Fair Isaac's Blaze Advisor™ business rules management system, ranked #1 in the *InfoWorld* Technology of the Year Awards). Typically financial institutions create and modify rules to add an extra layer of response to specific types of fraud incidents identified by case reviewers. If a new fraud scheme is showing up at San Diego ATMs, for example, a bank might add a rule to monitor certain types of transactions in these locations.

Adaptive Models improve responsiveness to current trends even further by automatically adjusting fraud scoring based on recent case dispositions. Layered onto standard models, they increase the sensitivity of the base model to changing behavior patterns based on the recent fraud/non-fraud activity that the standard trained model did not see in the historical training data.

For example, inventive fraudsters who know fraud detection systems are sensitive to CNP purchases of consumer electronics may start using counterfeit cards or stolen identities to buy college textbooks over the Internet instead. They can thereby "fly under the radar" of detection systems, and just as easily sell these goods "off the back of a truck."

Adaptive Models can nip the new scheme in the bud before visibility and losses have risen to the point where a rule will typically be written. In fact, they can begin to pick up the suspicious behavior based on just one or two disposed cases. As shown in the graphic below, while the base model may not be sensitive to the changing behavior pattern, the Adaptive Model will adjust the base score for any subsequent transactions with similar profile variable values upward so that it rises above the threshold for case generation.

FIGURE 7: ADDING AN ADAPTIVE LAYER TO A STANDARD FRAUD MODEL



In the same way, Adaptive Models also reduce the incidence of false positives (legitimate transactions receiving high fraud scores). Based on recent case dispositions, where behavior that scored high turned out to be legitimate, Adaptive Models can lower base model scores on subsequent transactions with similar profile variable values. The transactions would then fall below the review threshold, or at least be ranked lower in the review queue. Financial institutions would thereby focus analysts on more risky cases while lowering review costs and minimizing annoyance to customers.

Conclusion—be bold and aggressive, but be protected

Today's dynamic financial services markets offer financial institutions plenty of opportunity, and plenty of risk. While companies rush to bring innovative new offerings to their customers, criminals are rushing to exploit any and all vulnerabilities created by new processes, under-protected channels and changing customer behavior. Fortunately, financial institutions can lower their risk exposure by improving their fraud detection capabilities.

Fair Isaac, the leader and constant innovator in fraud management, has again elevated the state of the art in detection analytics. Today financial institutions can layer powerful, flexible new analytic capabilities—ideally suited to emerging markets as well as environments where customer behavioral data is sparse, unreliable or rapidly changing—onto existing transactional fraud detection. They can readily extend the Fair Isaac fraud solutions they currently rely on to protect their credit card portfolios into numerous other lines of business, including debit accounts and Retail Banking. They can also promptly deploy these techniques to cover Faster Payments and other accelerated settlement services, ensuring that these high-risk new channels are protected from the onset.

About Fair Isaac

Fair Isaac Corporation (NYSE:FIC) combines trusted advice, world-class analytics and innovative applications to help businesses make smarter decisions. Fair Isaac's solutions and technologies for Enterprise Decision Management turn strategy into action and elevate business performance by giving organizations the power to automate more decisions, improve the quality of their decisions, and connect decisions across their business. Clients in 80 countries work with Fair Isaac to increase customer loyalty and profitability, cut fraud losses, manage credit risk, meet regulatory and competitive demands, and rapidly build market share. Fair Isaac also helps millions of individuals manage their credit health through the *www.myFICO.com* website. Learn more about Fair Isaac at *www.fairisaac.com*.

Fair Isaac Corporation (NYSE:FIC) combines trusted advice, world-class analytics and innovative applications to help businesses make smarter decisions.

Corporate Headquarters:
901 Marquette Avenue, Suite 3200
Minneapolis, MN 55402
1 800 999 2955 *from the US*
1 612 758 5200 *from anywhere*
info@fairisaac.com *email*

Offices Worldwide:
Australia, Brazil, Canada, China, Hong Kong, India, Japan, Korea, Malaysia, Singapore, Spain, United Kingdom, United States

www.fairisaac.com

2439WP 01/08 PDF