Innovations in Debit Card Fraud Analytics

Stop Unchecked Fraud Growth by Expanding Visibility into Fraudulent Activity

May 2008

Summary

A healthy debit card market is cloaking an unhealthy rise in debit card fraud. The opportunity to steal cash, and take additional booty by accessing other accounts and services linked to demand deposit accounts is increasingly attractive to criminals, particularly as most PIN debit cards are underprotected.

This white paper discusses the need for PIN debit accounts to be managed with the same caliber of transactional fraud detection systems used for credit cards and most signature debit cards. It describes FICO™ Falcon® Fraud Manager for Debit, the latest version of which simultaneously detects the inherently different cardholder behavior patterns and fraud patterns associated with signature and PIN debit accounts. The paper also describes two advances that substantially improve fraud detection, speed response and reduce losses: integration of Falcon Fraud Manager for Debit with FICO™ Card Alert Service, a combination that boosts the performance of both products; and Global Profiling, a FICO analytic innovation which will be in the next Falcon Fraud Manager update.
In business, growth can sometimes mask big problems. For the payment card industry, rapid expansion in debit card market penetration and usage are leading to underestimation of the growing problem of debit card fraud. In fact, debit fraud on both signature and PIN cards is rising at a seriously fast clip.

The industry cannot afford to leave this growing fraud problem unchecked. When debit card market growth slows, as it inevitably will, the fraud rate is likely to continue to climb, causing fraud losses in basis points to soar. Fraudsters meanwhile, having been undeterred by weak defenses, will have developed and refined even more damaging techniques. Banks and card issuers must act now to avoid potentially huge losses, and the negative impact these losses would have on customer confidence and brand reputation.

The first step is to extend the same real-time transactional fraud detection that protects their credit cards and most signature debit cards to PIN cards as well. Banks and issuers using FICO™ Falcon® Fraud Manager for Debit to analyze signature-based transactions can direct their PIN-based transaction traffic through the same solution. The latest version of this product incorporates dual technology. FICO’s patented dynamic profiling technology captures inherently different cardholder behavior patterns and fraud patterns associated with signature and PIN debit accounts, enabling Falcon models to detect both types of fraud with a high degree of precision.

In addition, this white paper discusses two FICO analytic advances that lift debit fraud detection results even further:

1. **Integration of Falcon Fraud Manager for Debit with FICO™ Cart Alert Service.** While the Falcon system is focused on detecting fraudulent transactions on individual cardholder accounts, the Card Alert solution is focused on isolating and controlling large-scale card counterfeit losses. Integration improves detection speed and accuracy, and shortens response times, on both sides of the exchange.

2. **Global profiling in the next version of Falcon Fraud Manager for Debit.** Falcon Fraud Manager clients that upgrade will gain substantial performance improvements from being able to concisely and efficiently profile not only cardholders, but a wide range of other entities—ATMs, point of sale (POS) devices, telephone numbers, etc.—involved in card transactions.

Both of these solutions improve Falcon performance by providing additional transactional views that provide a more complete picture of fraudulent activity. When the two solutions are used together, their benefits complement each other. Banks and card issuers taking advantage of both these advances will have the means to stay ahead of the rising tide of debit fraud, keep the confidence of their customers and retain more of the profits from their expanding debit card portfolios.
Debit Fraud Update

Fraudsters find ways around protections—detection is more important than ever

Fraudsters are attracted to debit cards because, as outlaw Willie Sutton once said, "That's where the money is." Debit cards offer the prospect of not only making fraudulent purchases, but accessing cash from ATMs—no fencing or selling of goods required. Moreover as DDAs increasingly become the hub for other accounts and financial services, with new channels for using them emerging (e.g., online and phone banking), the potential value of the take from illegal account access further increases.

While PIN-based accounts still represent a much smaller percentage of debit fraud than signature accounts, they are attracting concentrated attention by counterfeiters and other fraudsters today. PIN accounts make a vulnerable target since fraud defenses on these accounts are generally less hardened than on signature debit and credit card accounts.

Fraudsters are finding many ways of working around the protections PINs are intended to provide. For example, with EPP-compliant ATMs now a requirement at non-financial-institution locations, criminals have stopped trying to steal PINs and other card information through wiretapping. But we're now seeing more instances of overlays being installed on top of keypads or tiny circuit board cameras being used to capture PINs, used in conjunction with skimming devices installed over cardreaders to capture card numbers. Fraudsters are also targeting more POS devices, especially at smaller merchant locations where older, non-EPP-compliant equipment may be in use or where network security may be lax or systems never intended for Internet exposure may be in use.

Even the chip-PIN protections deployed in the UK and other European Union countries have proven to be surmountable obstacles, simply requiring fraudsters to change their methods. While in the wake of chip-PIN, in-market counterfeit fraud has dropped substantially, cross-border fraud has surged. Fraudsters use the techniques described above to steal card numbers and PINS for manufacturing counterfeit cards, then use the cards for cross-border fraud in countries where magnetic stripe transactions are common. Stolen card numbers are also heavily used in-market for card-not-present (CNP) fraud, particularly online.

Meanwhile fraud patterns are growing more varied and ambitious. For example, fraudsters or their customers may sit on stolen cardholder data for months before attempting to commit fraud with it, but they may also use it within hours—at a location far away from the compromise site. Today they're also very quick in testing of stolen card data, with successful tests followed immediately by large withdrawals or purchases, often from another channel. For example, fraudsters may make a small online purchase or obtain a preauthorization through a bogus merchant account to determine that the card account can be accessed. They’ll then go to an ATM to empty out the checking account and any linked accounts they can get to. There was even a case recently of a multi-channel kiting scam involving accounts at several banks. Taking advantage of the two-day settlement window for ACH transactions, a fraudster kited ACH deposits by transferring funds from one financial institution's account to another. At the optimal moment for maximizing their take, they used ATMs to withdraw the funds. Total losses perpetrated by this ring amounted to more than $250K. While the perpetrators of such elaborate schemes could be lone fraudsters or small groups of independent operators—who today have access to unprecedented technology, outsourced services and secondary markets via the Internet—they're likely members of highly organized fraud rings, some of which have the global footprint and resources of a Fortune 500 company.
Two points of view are often better than one. When watching a sports event on television, for example, having more than one camera angle enables viewers to see aspects of game play and moves by the athletes that they wouldn’t be able to see with one camera.

This is the case with Falcon Fraud Manager for Debit and Card Alert Service integration. The two products have different points of view and different processes for achieving the same ultimate goal—to prevent fraud losses by detecting fraudulent activity as soon as possible.

When these points of view and processes are woven together, visibility into fraudulent activity increases, and both solutions become increasingly effective. Fraud detection speed increases, in many cases by up to 50 percent.

On the next page, you can see why. Figure sets 2a-c map detection and response processes onto timelines to show how these improvements occur through back and forth cooperation and how they accelerate fraud detection and interception.
Innovations in Debit Card Fraud Analytics

**FIGURE 2A: FALCON FRAUD MANAGER FOR DEBIT PROCESS—SOLO**

- Fraud starts
- Real-time fraud detection & case generation
- Case dispositions
- Fraud cards blocked & reissued
- Other cards part of the same compromise may show fraud activity days... or months later

**FIGURE 2B: CARD ALERT SERVICE PROCESS—SOLO**

- Transactional data received from ATM/POS networks
- Fraud/no fraud feedback from issuers
- Compromised Cards report to issuers
- Issuers block & reissue cards

**FIGURE 2C: CARD ALERT AND FALCON FRAUD MANAGER PROCESS—INTEGRATED**

- Confirmed fraud card numbers received as cases disposed
- Point of Compromise identification
- Compromised Cards report to issuers
- Cards on list blocked & reissued OR managed by Falcon Fraud Manager
Innovations in Debit Card Fraud Analytics

The debit fraud environment is becoming very complex as additional products and services are linked to demand deposit accounts and new channels emerge for card usage. It’s also increasingly dynamic, as savvy criminals frequently shift their targets and methods. A forthcoming version of FICO Falcon Fraud Manager for Debit will address this complexity by expanding FICO’s patented profiling technology to capture a broader view of debit transactions across lines of business and multiple channels. This advance also includes a mechanism for adapting profiling to changing fraud activity.

FICO’s dynamic profiling technology mathematically compresses immense amounts of historical behavioral data into highly predictive variables that facilitate real-time transactional analytics. Profiles enable models to examine intricate nonlinear relationships between many pieces of data in a fraction of a second to detect unusual behavior patterns.

<table>
<thead>
<tr>
<th>FIGURE 3: SUMMARY OF INTEGRATION BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Higher performance from FICO™ Falcon® Fraud Manager</strong></td>
</tr>
<tr>
<td><strong>More fraud caught.</strong> Card Alert makes Falcon Fraud Manager aware of fraud activity that does not look aberrant based on the transactional patterns of a specific account. For example, there’s nothing suspicious to Falcon Fraud Manager about a $200 ATM withdrawal from one account, but the transaction is suspicious to Card Alert because it’s one of 20 such withdrawals occurring on multiple accounts in a short time in a small geographical area.</td>
</tr>
<tr>
<td><strong>Quicker detection and response.</strong> Based on Suspect Activity Report from Card Alert, Falcon Fraud Manager can automatically generate cases for review. In this way, cardholders will be called sooner and fraud that might otherwise not be detected until the second or third transaction will be intercepted on the first transaction.</td>
</tr>
<tr>
<td><strong>Fraud loss prevention.</strong> Card Alert’s Compromised Cards list alerts FICO Falcon Fraud Manager to accounts where fraud hasn’t yet occurred but is likely to, enabling banks/issuers to act promptly to avoid these future losses. For example, they could block and reissue cards that look most risky based on recent Falcon Fraud Manager scores or write rules to deny transactions on the account without closing it (fraudsters who find they can’t use an account number will probably just move on and not revisit it). For less risky accounts, rules might tighten authorization conditions, causing a case to be generated, for example, if there is an attempt to make a large cash withdrawal.</td>
</tr>
</tbody>
</table>

» The Big Picture on Debit Fraud: Global Profiling

The debit fraud environment is becoming very complex as additional products and services are linked to demand deposit accounts and new channels emerge for card usage. It’s also increasingly dynamic, as savvy criminals frequently shift their targets and methods. A forthcoming version of Falcon Fraud Manager for Debit will address this complexity by expanding FICO’s patented profiling technology to capture a broader view of debit transactions across lines of business and multiple channels. This advance also includes a mechanism for adapting profiling to changing fraud activity.

FICO’s dynamic profiling technology mathematically compresses immense amounts of historical behavioral data into highly predictive variables that facilitate real-time transactional analytics. Profiles enable models to examine intricate nonlinear relationships between many pieces of data in a fraction of a second to detect unusual behavior patterns.
Falcon Fraud Manager for Debit currently creates account profiles to detect unusual cardholder behavior. In the future, it will also create Global Profiles to detect unusual behavior of other entities in financial services environments, such as ATMs, traditional swipe as well as contactless POS devices, mobile phones and telecom switches. These profiles are “global” because while they are involved in cardholder transactions, they are not specific to any cardholder account.

Global Profiles enable Falcon Fraud Manager to detect fraudulent activity that may not look suspicious from the point of cardholder behavior patterns alone. Because FICO’s advanced shared memory profiling techniques enable multiple profiles to be analyzed simultaneously by the Falcon models, visibility into fraudulent activity expands.

For example, as depicted in Figure 4, a debit cardholder’s purchase of $200 worth of jewelry from a merchant, while unusual, is not necessarily suspicious, and thus will probably not score above the threshold for review. What is suspicious is that a hundred similar purchases of jewelry have been made from the same POS device in the past day—and all with debit cards that have never been used with that merchant before. The fraud management system will detect this suspicious activity only if it is profiling both debit cardholders and POS devices.

The quantities of data involved in global profiling, even with the ultra-compression used, are potentially immense. Yet global profiling has a built-in way to minimize the number of profiles while maximizing the analytic benefit. As shown in Figure 5, dynamic analytic techniques determine, based on historical and current transactional activity and fraud patterns, which entities to profile. In fact, with each transaction scored, Falcon Fraud Manager for Debit determines if the entities involved are already being profiled. If so, it updates the existing profiles with any new information from the current transaction. If not, it determines if a profile should be created.
Innovations in Debit Card Fraud Analytics

FICO software innovations support this type of analytic innovation by making multiple-entity dynamic profiling immensely scalable. For instance, a leading UK telecom company, using multiple profiles to detect and predict network faults and revenue leakage, is analyzing over 1.5 billion transactions day in and day out.

Debit card markets will eventually become penetrated and revenue growth will no longer be able to cloak rising debit fraud, which is unlikely to slow. If fraud continues to grow at present rates, it will seriously cut into debit card profit margins. By the time that happens, debit card fraud is also likely to have become a huge customer satisfaction, public relations and political issue for the financial services industry.

By acting now to ensure that all of their payment cards are being managed with state-of-the-art transactional fraud detection, financial institutions will avoid the losses, costs and embarrassment of this scenario. By updating their transactional fraud detection systems with the latest advances, they’ll stay ahead of fraudsters who are increasingly focusing their ingenuity on getting at the cash and other prizes available through ubiquitous, underprotected debit cards. Once debit cards are subject to powerful transactional detection, like that which has brought credit card fraud rates down, criminals will find it much harder to reach these riches and their return on investment in fraud schemes will drop. Many will become discouraged and move on to look for other “low hanging fruit.”

**Conclusion—Act before Debit Fraud Becomes a Big Problem**

FICO software innovations support this type of analytic innovation by making multiple-entity dynamic profiling immensely scalable. For instance, a leading UK telecom company, using multiple profiles to detect and predict network faults and revenue leakage, is analyzing over 1.5 billion transactions day in and day out.
FICO (NYSE:FICO) transforms business by making every decision count. FICO’s Decision Management solutions combine trusted advice, world-class analytics and innovative applications to give organizations the power to automate, improve and connect decisions across their business. Clients in 80 countries work with FICO to increase customer loyalty and profitability, cut fraud losses, manage credit risk, meet regulatory and competitive demands, and rapidly build market share. FICO also helps millions of individuals manage their credit health through the www.myFICO.com website. Learn more about FICO at www.fico.com.