Divided we fall: Fighting payments fraud together

Mark N. Greene

It is a great pleasure to be addressing this august group. As some of you know, I began my career at the Federal Reserve back in 1982. So speaking to you is like a homecoming for me. I have been fortunate in my career to participate in the U.S. banking economy from three perspectives: at the Fed, obviously a policymaking central bank; at Citibank, a lender; and at two financial technology providers, including 12 years at IBM (International Business Machines) and the last year at Fair Isaac, a leader in decision management technology.

From these three perspectives, I have seen the tremendous collaboration that exists in the banking industry on the issue of fraud. However, from my current vantage point, I am also able to see a disturbing trend: More companies are declining to participate in some of these collaborative, consortium-based best practices. The reason is simple: They see a competitive advantage to keeping their information and experience to themselves. This raises some key issues for the financial services industry.

Do we want to fight fraud or move it around? That is, do we want to reduce the amount of fraudulent activity overall, or are we content to just have the most advanced banks move it to the less advanced banks, and to shift it from well-protected channels to less protected channels? Does a failure to maximize our effectiveness at fraud prevention have even deeper consequences? Which people, which groups, and which activities might we be funding if we allow fraud to persist? And are private industry initiatives enough, or is there a role in fraud prevention for public sector initiatives, mandates, or intervention?

I won't leave you guessing as to where I'm going with this. My experience has taught me the following.

- Fraud is too important to the economic and social well-being of our country to let it persist and grow.
- Individual gains must be balanced by the collective good.
- It is better to stop a fraudster than send him to the bank next door.

Now, my company is in the business of giving banks a competitive advantage. We have used consortium approaches to defeat fraud. We believe these collaborative approaches, along with ubiquity in protection, are essential ingredients in the fraud-fighting formula. They are necessary to reduce the "balloon effect" in fraud prevention, where progress in fighting a segment of fraud succeeds primarily in moving fraud from one place to another. We win when fraud loses—and fraud loses when we fight it together.

Types of payments fraud

Let me start by simply defining the key areas of payments fraud I'm discussing here. Fundamentally, we can divide fraud into two categories. There is first-party fraud, which is the abuse of account privileges by the account holders themselves, or the acquisition or expansion of those privileges by deceitful means. There is also third-party fraud, which is often identity fraud, or the abuse of one person's account by another. For the purposes of this talk, I am not discussing insider fraud, which is the misuse of a customer account by bank employees or others involved in the provision and distribution of financial services products.

First-party fraud typically involves your customer opening an account with you, with the intention of violating the terms of the account agreement. It can also involve a borrower selling his information to

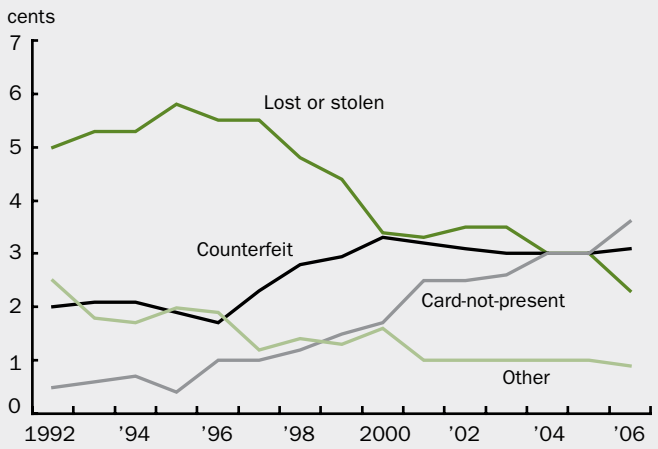
Mark N. Greene is the chief executive officer of Fair Isaac Corporation.

criminals or constructing a fraudulent identity or deceitful credentials for gaining credit. This type of fraud very often shows up in the collections queue as bad debt. But it is not traditional bad debt—when it is intentional, it is fraud.

Third-party fraud is what we usually think of when we consider fraud. This is stolen identities, the use of lost or stolen cards, and the counterfeiting of cards or other means of account access. It encompasses a wide range of techniques. This is where the criminal gangs operate—and where advanced technology comes into play to greatly reduce fraud losses.

FIGURE 1

Global card fraud per $100 in total sales



Source: HSN Consultants Inc., 2007, "Global card fraud," *Nilson Report*, No. 884, July, pp. 1, 6–7.

Fraud costs

Fraud—both first-party and third-party—is on the rise, but not across the board, according to Javelin Strategy and Research. That is because fraudsters are fast learners and attack less protected channels. Almost 4 percent of adult Americans were victims of fraud in 2007, resulting in losses of $51 billion. U.S. credit card fraud losses were down 22 percent to $11.4 billion; credit cards are highly protected by consortium models that are part of the Falcon fraud protection system. (I will talk more about that later.) By contrast, U.S. debit card losses rose 16 percent to $7 billion. Debit card transaction volumes are on the rise, and only some debit cards are protected by consortium Falcon models. Online purchase fraud experienced an increase, rising 33 percent in 2007. Though new account fraud incidents increased, total annual new account fraud losses dropped by 21 percent. There was a surge in new telephone account misuse, and existing checking and savings accounts fraud was up by 10 percent.

Just to take one example of a rising problem, card-not-present fraud (CNP fraud) is on the rise (see figure 1). It is estimated that about half of transactional card fraud today is CNP fraud. CNP fraud is primarily perpetrated through fraudulent use of cards for online purchases. CNP fraud is the biggest threat to online channels, such as PayPal.

Looking at global card fraud, we can see how the different methods of fraud have been changing over time. Certain fraud types are rising to "fill the gap" made by excellent progress in categories such as lost or stolen card fraud, since new technologies and channels enable new forms of abuse, as demonstrated by the rise in CNP fraud. To summarize, I have noted the following:

- We can make a huge difference by focusing on fraud in a collaborative way; and
- Fraudsters are moving from one channel and technology to the next, in what we call the balloon effect—squeeze them in one area and they move to another.

So are we winning the war on fraud, or just moving it around? We don't need any help recognizing the importance of fraud in its impacts to our businesses and the bottom line. But it is worth noting that real economic costs may be 150 percent of measured fraud losses. In other words, we are underestimating the problem when we just measure fraud losses. We know from our work with clients, for example, that a tremendous amount of bad debt is actually misclassified fraud. We worked with one prominent UK card issuer and found that more than 10 percent of the bad debt in its collections queue was really fraudulent activity. The costs associated with this is not just the charge-off losses; it is also the costs of having collections and recoveries staff and agencies try to collect unrecoverable monies.

Fraud's shifting focus

Of course, the costs to the lending institution and its customers are not the only costs we need to worry about. Terrorists and criminal organizations are funding crime through fraud. The costs here are incalculable. These costs make a strong case that a concerted, collaborative effort to fighting fraud is more important

FIGURE 2

Benefits of enterprise fraud solutions

Reduced fraud losses are seen as the chief benefit of an enterprise fraud solution

Note: All values are in percent.
Source: Theodore Iacobuzio, 2008, *Survey of Credit Card Issuers and Consumer Lenders: Connected Decision-Making for Collections, Risk, and Fraud Management in Turbulent Times*, TowerGroup, report, April.

than making fraud prevention a competitive advantage for a select group of lenders.

I've mentioned the balloon effect in fraud. The fraud detection and prevention tools that have been commonly applied by banks include card issuer and network transaction fraud solutions, a debit bureau and other identity protection for account opening, the implementation of chip and PIN (personal identification number) technology, the increasing usage of account verification techniques, and online fraud detection and transaction review tools. However, many new types of fraud have emerged or increased in response to the banks' defenses. These include the following:

- Increasing phishing and skimming attacks;[1]
- More attacks on small card issuers and smaller merchants that do not have the same level of protection;
- Recruitment of insiders to better enable fraud;
- Offshore fraud;
- Mail theft of cards;
- Large-scale abuse of card data retained at the point of sale;
- Declining effectiveness of address verification in detecting fraud; and
- International mail-order, telephone order, and online fraud.

The point here is that gains in one area of fraud are frequently offset by losses in another.

In fact, banks, retailers, telecommunications firms, and others are struggling to combat fraud, which is growing more complex all the time. There are more channels and lines of business to protect. There are regulatory mandates for better risk management. We are fighting sophisticated, worldwide criminal organizations. There are more frequent pattern changes. Lost, stolen, and counterfeit cards remain a concern, but we are also dealing with new forms of attack, such as Internet attack bots, which apply all kinds of techniques—persistence being the key ingredient—to work their way through online security measures.

Fraud solutions

Mass compromise losses could rocket higher given the low current criminal utilization rate of compromised cards. Large data breaches, to date, have been inefficiently leveraged by the criminals that end up with the information. Some incidents involving thousands of card numbers have resulted in only a few handfuls of fraudulent transactions. But breaches perpetrated by a more organized or effective criminal organization could have much more severe and immediate consequences.

The uneven protection of account types has raised interest in enterprise fraud systems. The information in figure 2 comes from a survey of leading U.S. banks conducted by TowerGroup for Fair Isaac this year. These banks are pursuing enterprise fraud systems as a way of controlling fraud losses. Today's fraud systems tend to protect one channel or product. It is like putting a burglar alarm on your front door but leaving the windows open. An enterprise fraud system is like a burglar alarm system for your whole house. This sounds simple, but it isn't. Few institutions today have the same level of protection across the organization. There are a lot of very well-protected doors out there—and some very open windows as well. As we discuss the importance of collaboration, it is important to understand that many of the principal victories that have been made in the area of fraud depend on collaboration. Next, I present three examples and focus on the collaborative aspect.

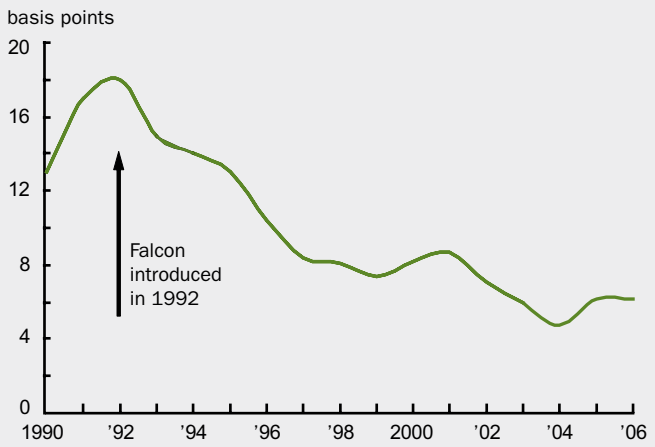
Falcon Fraud Manager

How does collaboration win today? It probably comes as no surprise that I'm starting with Falcon

Fraud Manager, which is a Fair Isaac solution. Falcon is an excellent example of the effectiveness of collaboration in fighting fraud. Falcon is the leading cards fraud protection platform. Falcon manages 65 percent of card accounts worldwide, including 90 percent of credit cards in the U.S. Falcon reviews card transactions and "scores" them based on their likelihood of being fraudulent, enabling card issuers to stop losses faster and to react dynamically to changing fraud activity in real time. Falcon's fraud detection is based on innovative neural network models that are "trained" on large sets of consortium data. These consortium models are embedded in end-user software or accessed by card issuers via third-party processors. The neural network models search through masses of data to identify very subtle signs of fraud. The size and diversity of the data are critical factors in the power of the models. We have created a fraud consortium that includes information on 1.8 billion card accounts, contributed by lenders that subscribe to the Falcon product.

FIGURE 3

Card fraud in the U.S., 1990–2006



Note: Falcon Fraud Manager is a leading cards fraud protection platform from the Fair Isaac Corporation.

Sources: Data complied by Fair Isaac Corporation, using information from HSN Consultants Inc., *Nilson Report* (various issues).

Falcon Fraud Manager typically cuts individual issuers' fraud losses by 50 percent and in many cases by more. But the really impressive thing is the impact this kind of solution can have on the industry. Falcon Fraud Manager was introduced in 1992, when card fraud was at 18 basis points in the U.S. As shown in figure 3, this number has since declined by about two-thirds based on the industry's use of a common, powerful fraud protection system.

This shows how a ubiquitous solution powered by close collaboration has served to benefit both individual issuers and the industry. Individual issuers have squeezed fraud out of their portfolios, and the industry as a whole has worked to squeeze a substantial amount of fraud out of the system.

Card Alert

Our second example involves automated teller machine (ATM) fraud detection. Some 11,000 banks in the U.S. subscribe to a Fair Isaac service known as Card Alert. What Card Alert does is trace the flight path of compromised cards to identify compromised ATMs. It works backward from compromised cards to identify whether they passed through a single ATM. The Card Alert team then identifies other cards that passed through the ATM in question. They notify the issuers that these cards may be at risk. The system currently flags roughly 500,000 unique card accounts annually as being compromised at ATM devices. So the information on card compromise from some issuers is used to benefit other issuers and to help criminal investigators.

Card Alert generates a wealth of data on ATM fraud trends, which is used by banks to systematically stop the fraud and by law enforcement to fight the fraudsters. Collaborative efforts like Card Alert have served to dramatically reduce the percentage of fraud that occurs at ATM devices.

Chip and PIN fraud

Our third example looks outside the U.S., to the chip and PIN rollout in the UK. This was an industry-wide, collaborative effort that resulted in nearly all devices being PIN-verified in the UK and, therefore, nearly all cards being much harder to counterfeit or scam. Over 90 percent of UK cards are chip and PIN cards now, and nearly 1 million retail tills have been upgraded. In 2005, this resulted in a 24 percent reduction in fraud from counterfeit, lost, and stolen cards, according to APACS (Association for Payment Clearing Services) in the UK.

However, while counterfeit, lost, and stolen card fraud has been contained by chip and PIN technology, it has pushed fraud for those same accounts to a new venue. Cross-border fraud—largely unprotected by the chip and PIN technology—went up by 43 percent in 2006 and by another 77 percent in 2007. Cross-border

fraud now accounts for 39 percent of all fraud for UK card issuers, compared with 27 percent in 2006. This shift swallows nearly all of the gains achieved through the reduction in fraud occurring in the UK itself. The problem that we're seeing here is that the collaboration worked in the UK, but because it was not executed in easily accessible neighboring countries, it failed to reduce UK issuers' overall losses. They decreased one form of fraud but increased another. Again, this speaks to the importance of both collaboration and ubiquity in avoiding the balloon effect.

Device and merchant profiling

How will new technical advances enable the industry to combat fraud? Let's look at three new advances that use payments data in different ways to increase fraud protection. The first is known as device profiling. One of the ways that successful card fraud solutions operate is to build a profile of each *cardholder* that can be used to identify unusual activity. By profiling *devices* as well, we are able to provide a more complete profile picture for a given transaction. The device profile looks for unusual device behavior: large amounts, rapid transactions, and suspicious patterns of transaction types.

Device scores can be combined with the cardholder scores to improve fraud detection. This approach can identify patterns that often involve multiple cards. It is especially useful in identifying counterfeiters and ATM burst fraud events. Device profiling requires a collaborative cross-issuer view, similar to the Card Alert service discussed before.

Our research shows a sizable predictive lift from adding cross-issuer device profiling. For example, there is an 80 percent relative performance lift in real-time value detection at a 10:1 false positive rate. This means that at a threshold where you are flagging ten "good" accounts to review for every one fraudulent account, you are identifying 80 percent more fraud than a traditional card system based on just cardholder profiles. If this kind of trade-off curve looks geeky to you, you have to understand that I am an econometrician working at a company populated by analytic staff. Geeky is where I work!

Our second innovation involves merchant profiling. As we discussed, today the standard is to profile *cardholders* and use every transaction to build and evolve the profiles. What we can do now is build a fuller picture by examining the *merchant* profiles as well. Merchant profiles are similar to cardholder profiles in that they contain a summarized view of detailed transaction information and history. They identify the points of sale that are more or less likely to experience fraud. The account fraud score is adjusted downward or upward based on the merchant information. This additional data collection increases the detection power of the model, through the integration of cardholder variables, merchant variables, and combined cardholder/merchant data. Better fraud detection means lower losses and improved customer service. Again, the ability to profile merchants effectively depends on the rich data coming from a cross section of issuers.

We have found that using merchant profiles in Falcon Fraud Manager, our card fraud system, enables clients to jump another level up in fraud detection. The enhanced version of Falcon, that is, with merchant profiles added, identifies substantially more frauds in real time, enabling the issuers to reduce fraud losses. At that same 10:1 false positive rate, the consortium subscribers are able to achieve a 40 percent relative performance lift in fraud detection and prevention.

Adaptive models

Our third example is a different kind of technology breakthrough. It involves what we term "adaptive models." The fraud models we have been discussing so far are based on consortium data, and every year we update the models by training them on the most recent set of consortium data. These new models are then used to upgrade our clients' systems. This has been very successful, but it means there is a lag time between the card issuers' experience of evolving fraud trends and the incorporation of that experience into their fraud-fighting tools. What we need is a way to capture new and important shifts in fraud patterns because of the highly dynamic nature of fraud.

The way *adaptive* models work is to adjust the model weights on each issuer's system. This dynamically tunes the models in response to actual fraud experienced by the issuer. This approach enables the issuer to benefit both from the broader view of fraud activity captured in the consortium model and from more immediate information on fraud against their accounts.

Our ability to detect fraud is increased with the adaptive models. Our research has shown an 18 percent relative performance lift in real-time value detection at a 10:1 false positive rate. These are just some of the advances coming in payments card protection. The point is that to make these kinds of advances, and to make them effective, requires collaboration. I have pled my case regarding collaboration.

Collaboration

What are the implications for the industry? The real frontline soldiers in the war on fraud—in particular the fraud managers who help protect their

institutions from a growing array of threats—need the best weapons we can give them. The innovations they depend on often stem from *independent* action and proprietary development. But these innovations are powered by *collaboration*. The trend toward viewing fraud management as a competitive advantage has potential negative implications for fraud management overall.

Models are stronger when they are trained on larger, more varied data sets. Certain types of information, such as device profiles, only provide value when powered by a macro-level view. And because fraud always finds its way to the weakest link in the chain, ubiquity helps contain the problem of the balloon effect.

So where might the public and private sectors collaborate next? Here is one idea: an industry-wide Fraud Alert Network. This would take the success of systems such as Falcon and Card Alert to a new level by building on collaboration. A Fraud Alert Network could take an approach to updating systems that is similar to the way companies such as AVG and Symantec fight computer viruses. By looking across millions of events, they are able to identify new virus patterns and automatically push updates to their user bases.

This is the model we are exploring for payments fraud. Rather than annual system or model updates, we would push out updates, rules, or hot lists automatically. The concept includes a *collaborative* rules subscription service, as well as simplified, timely consortium data collection. And the Fraud Alert Network includes a portal designed to bring banks, retailers, and others together to share ideas. Think of it as a private user community focused on real-time fraud issues—a Facebook for fraud management. In fact, this collaboration portal will go live later this month. We expect it to yield faster responses to fraud threats. It is a great example of where we see fraud protection going—toward greater collaboration and a real unified front. In summary, I leave you with these key ideas.

- Payments fraud remains a front burner issue.
- Fraud evolves with new payment product technologies.
- This is too big an issue to fight separately.
- Private sector collaboration is essential, as we have seen—it is really the foundation of the successful antifraud initiatives.
- Public sector involvement can help with best practices and information sharing.

In short, this is a war—divided we fall, united we win.

NOTES

[1]A phishing attack uses randomly distributed emails to attempt to trick recipients into disclosing personal information, such as account numbers, passwords, or Social Security numbers. A skimming device is one that is mounted to an automated teller machine or point-of-sale machine to copy encoded data from the magnetic stripe on the back of a payment card. For more information, see www.spamlaws.com/online-credit-card-fraud.html.