

Collections & Credit Risk

SPECIAL SECTION:
National Association
of Retail Collection Attorneys
Spring Collections Conference Guide

THE AUTHORITY FOR COMMERCIAL AND CONSUMER CREDIT PROFESSIONALS

www.CreditCollectionsWorld.com

May 2003 Volume 8/Number 5

Criminal Intent

A cross-industry fraud database is helping to identify repeat offenders. Can it - and other centralized databases - arrest the crime wave?

• **Collections Attorneys:
Hot Prospects and Hot Tamales**

• **Debt Buying:
Into the Mainstream**

• **Credit Risk Protection:
Is Demand Picking Up?**

Criminal Intent

By Jane Adler

A cross-industry fraud database is helping identify repeat offenders and prevent them from harming more people. But can it – and other centralized databases – arrest the crime wave?

It's estimated that fraud costs the financial services industry about \$35 billion a year. Much of the fraud takes place at the time of the credit application when the criminal uses a piece of stolen information such as a social security number taken from a wastebasket or a driver's license number lifted from a database. So it's hardly surprising that lenders are eager to find new ways to fight fraud.

Most creditors already use a number of tools – including credit bureau alerts and predictive models – to reduce their application-fraud losses. Moreover, fraud-prevention tools and products are constantly being reconfigured to stay ahead of inventive crooks. Recent innovations include Fair, Isaac and Co.'s addition of merchant information to its fraud-prediction product, Falcon Fraud Manager, and TransUnion LLC's new version of an identity-verification tool, TOTAL ID. And for its part, credit bureau Experian Information Solutions Inc. created the National Fraud Database, a whole new twist on fraud prevention. Created in 2000, the database compiles cases of known fraud from various lenders across several industries. The idea is to provide a quick way to stop fraud – especially in cases of identity theft.

Meanwhile, the government has been exploring how to create its own centralized database to fight fraud and identity theft. Several initiatives are underway, although turf fights among government agencies, combined with growing public fear that a truly national database of credit-type information would infringe on privacy rights, have marred early efforts. Experts think the only way to overcome those objections is to stress links between terrorism and identity theft. "Centralized information about fraud has to be part of the solution," says Fred H. Cate, a professor at the Indiana University School of Law in Bloomington, Ind. "Anything that helps centralize [fraud] information is a huge advantage."

A central repository of information is the backbone of Experian's National Fraud Database. The system contains known instances of fraud drawn from a number of industries. Creditors contribute information about fraudulent applications. In return, they can search the database for known fraud cases. "One of the basic premises of the system is absolute reciprocity," says Lyn Porter, vice president of fraud solutions at Experian in Costa Mesa, Calif. "You have to give to get."

The system has been operating in the United States for 18 months. Porter managed a similar system for Experian in the United Kingdom, which has been running now for 12 years. (Experian is a subsidiary of U.K.-based GUS plc.) Porter notes the

Fair Credit Reporting Act regulates the U.S. system. "That gives clients protection [from being sued] as long as they don't knowingly report inaccurate data," she adds.

Creditors that contribute to the Experian Fraud database must conform to stringent reporting guidelines, according to Porter. That ensures the records are accurate and verified as fraudulent. "We have the gold standard in verified and pristine fraud records," she says. Members must also agree to manually review accounts that appear as possible frauds. "That's where victim alert-type systems fall down," says Porter. "Lenders don't always review those accounts that are flagged."

Although Porter emphasizes that the system is designed to serve small as well as large firms, so far a handful of big companies are using the Experian database. They include such marquee names as Sprint, Capital One, Toyota, American Express, First USA/Bank One, and Dell Financial, the finance arm of Dell Computers. The database currently has about 400,000 records, about half of the files are from telecom companies, and it currently serves primarily grantors of consumer credit. But Porter says the company is "in the process of setting up a commercial user group," which she expects to have working later this year.

Cross-Industry Tool

Among fraud detection tools, the Experian database stands out because it includes multiple industries, according to consultant David A. Poe, managing partner at Edgar, Dunn & Co., San Francisco. He says the fraud product that most closely resembles the Experian database is Issuers Clearinghouse Service, a joint venture of Visa and MasterCard. But that system includes only information from credit card applications. "The addition of other types lenders is useful," Poe says.

Poe found this to be the case in an independent study he conducted on customer authentication by credit card issuers. He says telecom fraud was a



"If fraud has been used for a mobile phone, that's an indicator that fraud has been used for a credit card too."

***David A. Poe
Managing Partner
Edgar, Dunn & Co.***

predictor of credit card fraud. In other words, criminals used fraudulent information to get a cell phone and then applied for a credit card. "If fraud has been used for a mobile phone," Poe says, "that's an indicator that fraud has been used for a credit card, too."

Early results from the Experian system seem promising. Last September, the company published the findings of an internal study that showed applications with a match in the database were at least seven to 12 times more likely to become frauds than other applications. In one test, fraud rates on database matches were as high as 90%. "Clients are seeing benefits and payback," says Experian's Porter.

That seems to be true at Sprint Corp.'s wireless division, which has been a National Fraud Database user for about a year. After activation, accounts are matched to the database. (Sprint uses other fraud-prevention tools, too.) As a result, fraud losses have declined by about 50%, reports Sherlyn Renner, director of fraud management at Sprint in Overland Park, Kan. And the length of time a fraudulent account is active has been reduced by 51%.

The availability of fraud data from other industries has helped. Credit cards provide the second highest number of fraud hits. "We are zeroing in on the food chain of fraud," Renner says.

Sprint recently initiated a pre-activation trial of the system in five markets. Though still in the early stages, test results have provided "lift," or additional fraud catches, says Renner, although she declines to provide any actual numbers.

Another user of the National Fraud Database is Dell Financial Services L.P., an Austin, Texas-based joint venture of Dell Computer and the CIT Group. Credit applications are checked in real time because most Dell products are bought over the phone or online.

Online fraud is a growing problem. More than \$700 million in online sales were lost to fraud in 2001, according to technology research company Gartner Inc., Stamford, Conn. And online fraud losses for 2001 were 19 times as high, dollar for dollar, as fraud losses resulting from off-line sales.

At Dell, an application that gets a match in the fraud database, such as an address or phone number, triggers a review. The applicant is asked questions that can verify identification. "We try to make the questions the least intrusive for the customer," says Roger D. Kidwell, vice president of risk management at Dell Financial.

Dell uses a number of fraud detection tools, but Kidwell believes the National Fraud Database detects fraud that other systems can't. "Catching fraud is like finding a needle in a haystack," he says. "It's all about false-positive ratio management, and this really helps you focus on certain applications."

Kidwell won't share actual results, but he will say that hit ratios vary depending on the configuration of rules for matches. Some rules may target only phone numbers. Others may include a host of variables, such as name, address, and phone number. "Like any fraud tool, you can tighten the rules or make them loose," he says. "You can get precise or throw the net a little wider." He warns, however, that if rules are drawn too tight, cases of fraud might be missed because criminals often use only one piece of fraudulent information.

Companies that participate in the National Fraud Database pay a monthly

fee, plus a per-inquiry cost. Costs vary depending on the volume of accounts and mode of access. Possible access modes are similar to bureau-based fraud tools. Experian's Porter says a high-volume user, say about 10 million inquiries a year, will pay single cents for a report.

Although Kidwell at Dell Financial won't say how much he pays, he agrees that the start-up costs are "not too high a barrier." To improve efficiency, Dell pulls the fraud inquiry at the same time as the credit bureau report.

More is Better

The National Fraud Database has 12 clients and Porter says there are about 20 others in the pipeline. But she admits more contributions would make the system better. "The greater the participation, the more fraud you can find. Then the more losses you avoid and the more consumers you protect," she says. Kidwell at Dell Financial, who also co-chairs a board that oversees the National Fraud Database, encourages all types of other creditors to participate. "The more people who share data, the better," he says.

The addition of a new data source has increased the effectiveness of Fair Isaac's fraud predictor, the Falcon Fraud Manager, according to Timothy J. Grace, vice president of business management for fraud analytics at the San Diego office of Fair, Isaac.

The company recently completed its first pilot program to add merchant information to its database. "We got a 10% increase in detection levels of fraud," Grace says.

Meanwhile, interest has steadily been growing to create a master database that would share all kinds of information. The FBI has a database of Internet crime that includes some credit card fraud and cases of identity theft.

The Federal Trade Commission already has a

clearinghouse, or database, of identity theft victims. It was created after Congress passed the Identity Theft Act of 1998. In operation for three years now, the database has about 300,000 complaints so far. These include complaints to the Social Security Administration about the fraudulent use of numbers.

The FTC is considering a pilot program to test whether information could be shared with credit reporting companies, according to Joanna Crane, program manager at the FTC's Identity Theft Program. "We are not sharing data yet," Crane says. "But we are working toward sharing this information." There's no time line for the project, but, she says, some type of national database would be a terrific law enforcement tool. "Everyone is interested in this."

That may be true, but there's little consensus about what form a national database would take, who would contribute, and how it might sidestep legal and privacy issues. "If the right business model were found, there could be huge advantages," says Michael O'Connell, senior director of product development and management at Chicago-based

TransUnion, which has a number of fraud products including an assistance center that logs consumer complaints. He thinks such a database would need to be a joint effort among credit reporting agencies and financial institutions. "If the databases have different information, there would be some [advantage] in combining sources."

There are huge impediments to the creation of a truly national and comprehensive fraud database, experts say. Notification of consumers regarding the sharing of their information might be an insurmountable task. Another big obstacle is that sharing data might violate privacy laws.

The real problem isn't how to centralize information, but the existence of too many fraud databases, according to Washington, D.C., attorney Helen Goff Foster at Bryan Cave LLP. Infighting for data among government agencies has hampered progress.

New Legislation

Also, new federal legislation on identity theft is expected to be linked to FCRA provisions that expire at the end of the year. No one knows exactly what shape a new law might take and how it might constrain efforts to create new fraud databases. But the legislation would probably include additional penalties for identity theft, experts say. Suggestions have also been made that creditors might be penalized for not investigating a file with a fraud alert.

Last year, California enacted a new law that allows consumers to put a fraud alert on their credit file even if no fraud has been committed. "It's a little troubling," says law professor Cate. "Lenders are not thrilled with this."

In the end, the only answer may be for the Department of Homeland Security to create a central database to stop identity theft because of worries about terrorism. Says attorney Foster: "If you assign the job to one agency with real authority, then you could talk about developing a comprehensive national fraud database." ■



"We are zeroing in on the food chain of fraud."

*Sherlyn Renner
Director
Fraud Management
Sprint Corp.*