Battling Cyber Fraud

By Karen A. Frenkel

Last August, law enforcement officers arrested Texas diamond dealer Michael Burke and charged him with laundering more than $100,000 worth of stolen diamonds. He and seven others allegedly stung etailers with fraudulent credit card information, specifically identity theft. Last spring, a Russian crime ring recruited middlemen to order thousands of dollars worth of diamonds online and may have hacked into a bank system to input the intermediaries' addresses on credit card records. When the loot arrived at their homes, they reboxed it and shipped it to Russia.

Unlike their brick-and-mortar counterparts, e-jewelers own the risk of credit card fraud. If a customer walks into a store, purchases with a credit card, and the merchant authenticates it, the merchant gets paid by the card issuer no matter what. It is far more vital, therefore, for virtual jewelers to reduce fraud by knowing their customers and flagging high-value orders with a variety of tools.

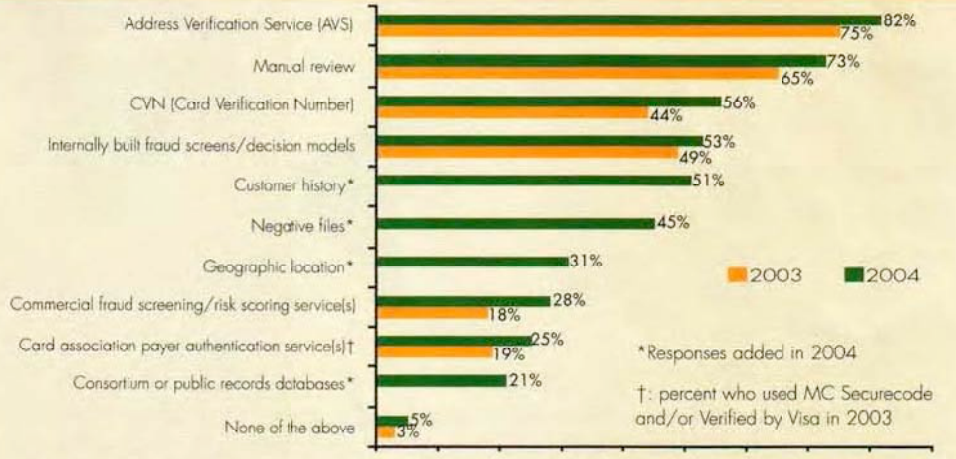
DOUBLE WHAMMY

One site hit by both the Texan and Russian operators is DiamondSafe.com, which is owned by Lieber and Solow, Ltd. In March 2002, a customer phoned in an order on the site for a ring worth almost $19,000. Six months later, Marcy Friedman, who processes DiamondSafe.com's orders, became suspicious when she recognized the perpetrator's thick Southern accent as he ordered a $15,000 loose diamond. DiamondSafe awaits a court ruling on the case. The Russians bested Friedman when the same customer ordered two costly items back-to-back through the site. For the first, a pair of $4,600 earrings, the billing, shipping address and security codes all matched the card. Then he ordered a $5,000, three-stone ring and called several times to expedite the order with overnight shipping and to check the status. That, and his thick Middle Eastern accent, alarmed Friedman. When she doublechecked, she noticed he had used a business credit card with a personal residence address in Minnesota. Friedman tried but was unable to stop delivery to the U.S. address or to prevent the shipment from going abroad. Various law enforcement agencies she contacted said the dollar amount of the transaction was either too small or too large for them to intervene. And mail delivery service representatives said that either it was too late to stop delivery or the matter was outside their jurisdiction.

Fraud Management Tools Used

2004 Question: What types of process(es) and/or tools does your company currently use to manage online payment fraud, including credit card fraud and other fraud?

2003 Question: What types of process(es) and/or tools does your company currently use to manage online credit card fraud?



Source: 6th Annual Fraud Survey © Mindwave Research & CyberSource 2004

UNWITTING COLLABORATORS

"Transshippers," who handle the reboxing of the item for shipment to the final destination, are a major concern of jewelry etailers, according to Victor Dolcourt, senior product manager in risk products for CyberSource Corporation, which provides secure electronic payment and risk management solutions to etailers. "Fraud perpetrators won't get diamond merchants to sell to Eastern Europe, but they can get them to sell to individuals here," he says. These sophisticated fraud rings find unwitting collaborators through online work-at-home sites, bulletin boards or dating services. Then they impersonate legitimate credit card holders or hack into card issuers' systems to change the names and addresses, or portions of addresses, of legitimate credit card account numbers. Finally, they have orders shipped to the intermediary and ultimately sent to the crime ring's foreign address.

Many jewelry etailers are just as vulnerable as DiamondSafe.com. According to Doug Schwegman, director of customer market intelligence for CyberSource and author of its annual fraud survey, last year jewelry etailers lost $48 million to fraud, or 1.8 percent of $2.8 billion, the total online jewelry sales. With online jewelry luxury goods sales poised to grow 31 percent this year, according to Forrester Research, will fraud rates rise too? According to Schwegman, jewelry etailers experience the same fraud rate as all etailers. That rate flatlined for the first time during 2003 and 2004 but when the same 1.8 percent fraud rate is applied to increased sales dollars, proportionally greater dollars are lost. "Assuming the same percentage loss this year and a 27 percent increase in online jewelry sales, fraud loss could reach $61 million, or 1.8 percent of $3.6 billion," says Schwegman.

While all etailers have the same exposure rates, e-jewelers and electronics vendors have characteristics that render them particularly conspicuous and enticing to fraud perpetrators. Dolcourt says that "both sell big-ticket, fenceable items." The average value of all fraudulent orders reported by 348 etailers in CyberSource's 2004 survey was $800, whereas the nine participating jewelry etailers averaged orders of $1,900. "Most fraudulent orders are 50 percent higher than the average order, but fraudulent jewelry orders are 140 percent higher," explains Schwegman. "Jewelers get ripped off for more than average merchants."

Fraud perpetrators use web crawlers, programs that ferret out sites with many transactions and expensive items, so mid-level jewelers with an annual $40 million in transactions of items costing more than $1,500 are likely targets. It also is easier to hide mid-price-range products on auction sites. For example, it's easier to sneak through a $2,000 necklace than a $40,000 one.

DEFENSE TACTICS

How can the jewelry etailer protect himself? One way is to get to know their customers so they can trust the orders they place. DiamondSafe.com's Friedman checks all orders manually, but when one comes in over a certain amount, she uses an independent payment verification system to check identities. While on the system's website, she calls to verify the buyer's name, address, the last four digits of their

High-Risk Online Fraud Areas Outside U.S./Canada

Riskiest Countries

3%+ mentions shown

#1	Nigeria	31%
#2	Indonesia	8%
#3	Russia	6%
#4	China	5%
#5	Afghanistan	4%
(tie)	United Kingdom	4%
#6	India	3%
(tie)	France	3%
	Mexico	3%
	Romania	3%
	Vietnam	3%

Question: From your experience, which single country outside of the U.S. and Canada poses the highest risk of online fraud (i.e. in your experience, orders from this country have the highest probability of being fraudulent)?

Source: 6th Annual Fraud Survey © Mindwave Research & CyberSource 2004

Social Security number and other information and types that into the online form. The system does a security check and then tells her if the customer passed or failed. Once she gets the go-ahead, she uses PC Charge Pro software to process the order and automatically deposit the transaction amount into DiamondSafe's bank account.

Friedman declined to name the verification system, but chose it because she finds some credit card companies less helpful to businesses and more customer-friendly. "They still verify addresses, but some will no longer check security codes. They're concerned about infringing on customers' privacy," she says. She asks those cardholders to fax copies of their driver's licenses and credit cards. "If their intention is fraud, they get scared and hang up," she says.

CyberSource's Dolcourt disagrees that company cards are becoming less helpful to merchants. "They provide less information," he says. "MasterCard and Visa offer a standard pay authentication service that merchants can put on their sites so that customers can identify themselves with a Personal Identification Number." These card issuers combined forces and introduced MasterCard Secure Code and Verify by Visa two years ago. Merchants resisted the standard at first, because they had to reconfigure their sites and the checking-out-process requires one more step from customers. Friedman does not find the process very user-friendly. "It seems difficult to install and requires us to change internal company programs," she says, "Customers aren't even that familiar with security codes and if they have to input a PIN, that makes it even more difficult. They may just as well go back to real stores." But Dolcourt says the system has caught on in the last six months and that two or three diamond merchants are successfully implementing it.

CyberSource offers a hosted service that incorporates Visa's intellectual property to help validate that a customer is really the ultimate consumer. Information that seems unrelated may flag a transaction as more prone to fraud, so CyberSource's 200 detectors correlate facts and convert them to 8,000 fraud tests. Merchants rent the service on a transaction basis and can change parameters quickly, a considerable advantage because fraud is dynamic, and morphs day-to-day. The system also tests information technology (IT) protocols to determine what server an order originated from. If it arrives from a foreign country, but claims to be American and has a United States billing address and telephone number, CyberSource notes that inconsistency. "We don't blackball areas, but we do give more weight to some physical locations based on the history of fraud there," says Dolcourt.

But in the effort to reduce their vulnerability to fraud, merchants run the risk of insulting their customers and rejecting legitimate business. And even with her fraud-prevention systems in place, Friedman routinely flags $300 orders that turn out to be attempted heists. Fraud perpetrators "put a lot of effort into their scams. This is their day job," says Dolcourt. The fraud rate plateau may therefore be temporary. "It's a see-saw battle," says Schwegman. "Fraud perpetrators get smarter and they specialize. But merchants are clever too. It's crucial for online merchants to reduce fraud, but they can trust their customers while being very alert and using lots of tools." ✦

High-Risk Online Fraud Areas Within U.S./Canada

Riskiest Areas - U.S./Canada

2%+ mentions shown

	STATE		CITY	
#1	New York	26%	New York City	26%
#2	California	17%	Los Angeles	9%
			Bay Area	2%
#3	Florida	15%	Miami	10%
#4	Michigan	3%	Detroit	3%
	Illinois	3%	Chicago	3%
	Canada	3%		
#5	Texas	2%		
	Pennsylvania	2%		

Question: From your experience, what single major U.S. or Canadian metropolitan area poses the highest risk of online fraud (i.e. from your experience, orders from this metropolitan area have the highest probability of being fraudulent)?

Source: 6th Annual Fraud Survey © Mindwave Research & CyberSource 2004