



Friday, July 6, 2007

## **Sharing Data, Protecting Business**

by Emily Swoboda

The top five digital threats to e-commerce, according to *Forbes Magazine*, are as follows: transaction fraud, outside hackers, inside hackers, sloppy software and using laptop computers. In the online gaming industry, data sharing can create a formidable defense against fraudsters. So, why are banks and credit card issuers still not quite on board with the idea?

Three professionals from different areas of the payments sector discussed last month the evolution of data sharing and what still needs to be done to prevent fraud in the worlds of e-commerce and online gaming.

Andre Edelbrock, president and CEO of data sharing and fraud management firm Ethoca Systems, said fraud continues to keep up with merchants. So, as merchants implement one security technique, fraudsters learn techniques to get around them.

"They will learn ways to go around that and take advantage of that," Edelbrock said. "And it forces the merchants to go one step further. So, merchants know that as their lifeblood--deposits and such--continues to grow, fraud is going to continue to grow right along with it. So, merchants are now turning to working with each other to share information because the first thing they check is: 'Well, I've been through this; I've been used before; I've been subject to a chargeback.' So, the natural next step for them is to say: 'If this happened to me it could happen to somebody else.'"

Alberto Espana of Xstrategies LLC, a U.S.-based financial strategy and payments consulting firm, said there is more of a trend in data sharing between merchants and acquirers, such as payment processors, than with banks. On the one hand, data sharing is an important practice for merchants to engage in, but banks and issuers should be involved as well.

"It's a good practice--if a merchant sees somebody come to their Web site and use 10 different credit cards, you should let your acquirer know," Espana said.

Andrea Wilson of Bermuda-based payment processor First Atlantic Commerce said the industry has systems designed to protect acquirers, but they aren't working as well as they could because the rules they have set up are archaic and don't fit with today's progressive technology.

"They have a reporting system called SAFE," Wilson said. "And, basically, what you're supposed to do as an acquirer is if a merchant has fraud or high chargebacks you're supposed to report them to the issuers. It's for statistical tracking, but as a non-registered member of these private associations, I cannot gain access to that information and (as the payment processor), I need that information more than anyone. The acquirers have it, but they don't share it. This is where we start to see elements in the industry where there is not a lot of cooperation because Visa and MasterCard said 'You're not a member? You don't get the information.' And it becomes a real problem when you try to assist in fraud litigation because they have access to the information, but you're not allowed to because of the rules, which are outdated."

A recent study by Colorado-based First Data Corp. of the global banking industry found that while most agree there is a need for data sharing, there are significant barriers that stand in the way of such collaboration.

According to the study, 96 percent of the respondents, who hailed from 52 banks from around the world, believe that fraud is perpetrated on a global stage, learned and passed from one part of the world to another. This would appear to support the need for data sharing to prevent fraud on a global level, but the opinion of one respondent indicates otherwise.

"Organizations are secretive of fraud losses and that inhibits our ability to work together," the respondent said.

On the other hand, there is some progress in the bank-merchant-processor arena. The Royal Bank of Scotland announced in June that Ethoca will provide it with data sharing services in relation to e-commerce.

### **Phishing and Card Testing**

Fraudsters can acquire credit card numbers from legitimate cardholders by sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Testing involves using a card number on various sites to figure out whether a card will authorize or not.

Espana said unfortunately there is very little a merchant can do to prevent a customer from saying "It wasn't me." Furthermore, a merchant cannot stop a merchant from declining a transaction. The danger lies in establishing a pattern because it damages the merchant, not the fraudster.

"If your Web site is considered OK by an issuer bank and a fraudster finds that out, they will use their Web site to test it out before they go and make purchases in the real world," Espana said. "And when the issuer sees a trend form, they won't wait for it to happen again--they will just go ahead and block your Web site. And no matter what you do, anytime a transaction comes through that Web site it will be declined."

Wilson offered a simple but poignant piece of advice on data sharing and its role in the security of e-commerce.

"You only have what you've experienced; you don't have what everyone else has experienced," Wilson said. "So, that is why data sharing is so important."