

WASHINGTON OUTLOOK



ISO CONCERNS

by Jim Romeo



Jim Romeo is a regular contributor to Transaction World Magazine and is a freelance writer based in Chesapeake, Virginia who specializes in business and technology.

As of this writing, Congress is considering legislation in both the House and the Senate that would stall reforms aimed at curbing swipe fees - before they even take effect. (Note: at press time the Senate has voted not to delay the implementation of the reforms while the House vote is still pending.)

Last year, Congress passed, and the President signed into law, important bipartisan reforms aimed at fixing the current interchange system, as part of the Dodd-Frank Act. As a result, new rules requiring that debit card swipe fees are reasonable are set to take effect this summer—but the big banks and credit card companies are fighting hard to protect their cash cow, by seeking delays. This is a topic of concern nowadays, depending on which side of the transaction chain you are on. But another problem lingers—it's called the economy. So how exactly is the present state of the U.S. economy affecting the market for card transactions?

"Recent year over year trends have shown card transactions declining slightly as a large number of consumers affected by the economy have been attempting to be fiscally responsible," says Tsion Gonen, Corporate Vice President, Products and Marketing for SafeNet, located in Belcamp, Maryland. "Similar trends have also been seen in Europe. However, as the economy starts to recover, the market is poised for incredibly fast growth. We're seeing the introduction of more convenient payment methods and advances in mobile commerce that are making it easier than ever for consumers to make card purchases, anytime, anywhere."

Much future growth hinges upon consumer confidence and trust. But trust hinges upon peace of mind that a security breach is unlikely.

"As the economy recovers, transaction levels grow so consumer confidence and convenience of electronic transactions versus cash and check, drives higher card usage," says Chris McNulty, Sales

Director for Payments, for Voltage Security. "This continuing increase in dependence on the electronic payments further emphasizes the need for ongoing improvement in processes and protection of data within that ecosystem."

If the economy is seeing the light at the end of the tunnel, how do things look for ISOs? ISOs have long been seen as a de facto consultant to the merchant, knowledgeable in technology and security issues, giving them assurance that their transactions are secure and also helping them expedite their transactions with the latest technology.

"The outlook for ISOs is good," says John Barrett, SVP of Independent Sales Service at First Data, based in Atlanta. "There is opportunity in the payments industry for ISOs and agents who are on top of the trends and can help merchants create opportunities and solve problems. Ideally those conversations go beyond transaction fees and focus on building value to the merchant's business. Helping a merchant address data security issues or implementing a gift card program that increases foot traffic can help ISOs increase merchant retention - something that's critical in any economy."

Because merchants have always moaned and groaned over interchange fees, the ISO can be an excellent source of information and knowledge on technology issues that can help them process sales and revenues through electronics more efficiently.

"ISOs and other transaction processors need to work on two fronts: implementing the latest technology to create new efficiencies and being in the fore front on security issues," says Sam Alapati, Senior Technical Director for Miro Consulting. "Efficiency and technology should both be treated equally with the same amount of priority. The economy does affect technological upgrades and a revamping of security, but these are not options - one must innovate and be highly secure, or they may perish."

"As business-to-business card payments continue to grow, I believe we will see the financial performance of ISOs and others in the transaction processing industry increase as well," says Mike Kresse, SVP of Payment Services for SunGard AvantGard. "But more than that, I think there is a unique opportunity to rethink traditional models of processing card payments. This is a great opportunity for innovation - whether push payments and the opportunity to solve the problem of requiring the vendor to get a new MID, or equipping vendors to pass Level III data so that they capitalize on lower interchange fees."

For ISOs and others in the card transaction industry, there's always fear in a tumultuous environment that something is brewing somewhere that could affect their business. So is there an "elephant in the room" in the card transaction nowadays? We asked.

"Clearly the 'elephant in the room' is related to interchange fees," says Mike Kresse of SunGard AvantGard. "By definition, an 'elephant in the room' is something not talked about. Interchange fees and rebates are talked about, but revenue models for the ISOs and Issuers are not. I believe that vendors often miss the fact that the infrastructure required to support card payments comes with certain costs - and that those costs need to be paid for. In return for that cost, vendors receive a guaranteed form of payment without having to expose their bank account and routing information. But what we see that is most often missed is that with card payments, vendors do not have to expend the cost that is required to process an individual check. Card payments are truly the quickest, most secure, and most easily integrated electronic payment solution for business-to-business payments in the market today. That is because a very robust and elegant infrastructure, costly as well, exists to facilitate that."

ISO Concerns

Continued from previous page

Aside from security, many in the industry
**SEE THE APPLICATION OF TECHNOLOGY
 TO SUIT THE NEW CONSUMER HABITS
 AND LIFESTYLE**
 as a quiet opportunity that has not quite been exploited.

Chris McNulty sees confusion on security issues and a subtle laxity when it comes to security.

“I see a lot of confusion around encryption versus tokenization and how EMV may impact data security,” says Chris McNulty. “All vendors should be focused on enabling their systems or devices to allow for end-to-end encryption and tokenization as needed. As EMV comes to the U.S., it will help reduce fraud but does not eliminate the need for encryption to protect the data. In my opinion, too many Level 1 merchants are waiting for more detailed guidance from regulatory authorities around PCI compliance when they should be focused on proactively implementing data security technologies such as encryption to protect their customers and brand reputation. A secure environment will always help with compliance and more importantly, protect against breaches of all sizes. Ignoring these problems will not make them go away – the time to be proactive is now.”

Security threats and vulnerabilities are becoming more sophisticated and that means that ISOs always have to be up on the latest security trends and technologies.

“It is no longer enough to protect the back-end of your payment infrastructure. As security attacks become more sophisticated in nature, ISOs can’t rely on the standard security protocols that worked in the past,” says Tsion Gonen. “They must protect the entire system, down to the data level, and ensure there

are adequate security measures in place in the front-office, beyond a username and password, to control who is accessing the systems. Recent breaches have highlighted the ease with which usernames and passwords can be shared with third parties, who can then infiltrate a vendor’s system. ISOs need to look at how they can build a trusted environment, where users are properly authenticated and all cardholder information, not just the credit card number itself, is encrypted. This way, if someone does access an ISO’s system, all of the consumer information is protected.”

“The industry has definitely made great strides toward efficiency and security,” says Gonen. “Data breaches related to credit card security have dropped significantly and consumers are feeling more confident with their credit card purchases both online and at retail establishments. Card technologies have no choice but to continue to make advances in performance, convenience options, and security to keep up with growing consumer requirements and expectations.”

Aside from security, many in the industry see the application of technology to suit the new consumer habits and lifestyle, as a quiet opportunity that has not quite been exploited.

“Payments technology is evolving quickly, and that means new opportunities for ISOs,” says John Barrett. “Merchants who purchase multiple products and solutions are less likely to leave when a competitor walks in the door

offering a lower price. There is significant momentum around paying and accepting payments with a mobile device and, that means opportunities to sign new merchants and help existing ones be ready for wider adoption.”

The wide array of technology even opens the door to ways of customizing applications and technologies according to the industries and applications which the ISOs serve.

“From pre-paid, to single-use cards, to the various ISOs and transaction processors, I believe there is more opportunity than ever to bring custom-tailored solutions to payer organizations based on their individual needs,” says Mike Kresse. “Never before have we been able to approach companies with so many options based on their individual requirements.”

Kresse also believes that vendors are increasingly concerned about PCI-DSS compliance and the risks involved in holding onto card information. “Vendors look to their ISO to advise them on how to minimize the risk of this data becoming compromised,” he says. “I believe that vendors are looking beyond just the fee structures that each ISO is offering, and I see that ISOs have an opportunity to differentiate themselves by offering a more consultative approach to card processing – whether discussing push payments or providing solutions where they take on ownership of the card data for the vendor – for example.” ■