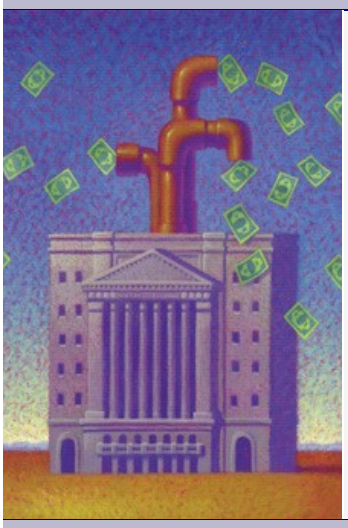

Living in a Card World Where Technology Changes Every Day

by Jim Romeo

A year after federal credit card reform legislation went into effect, Elizabeth Warren, the Obama Administration's head of the newly created Consumer Financial Protection Bureau, stated publicly that the legislation is effective and, in fact, warned against over regulating within the industry.

"A study recently issued by the Consumer Financial Protection Bureau reviewed certain aspects of the cardholder experience, including, for example, fees and rate hikes and various issuer policies," says Donna L. Wilson, a partner with the law firm of BuckleySandler LLP, in Los Angeles, California. "According to the CFPB, the results of the study indicated that, for example, cardholders are paying less in late fees. What the study did not review, however, was whether the new regulatory framework has made credit less available to riskier customers. For the foreseeable future, it should be expected that legislators and regulators will continue to pay close attention to the credit card industry."

But the jury is still out as to what legislators are thinking. "Two of the biggest issues are technology and increasing regulation," says Wilson. " For example, the advent of mobile payment systems will raise a host of issues -- in terms of business models going forward, privacy and data security and the like."

Robert Livingstone is President and Founder of Ideal Cost, West Palm Beach, a Florida firm that consults with businesses on how how to reduce their credit card acceptance fees concurs. "The biggest technology trends are clearly in mobile payments," he says. "Using one's cell phone as a credit card is certainly coming soon as it is already prevalent in Europe and Asia. Also, accepting payments by mobile phone is also growing rapidly, especially in practice by Square. The biggest concern ISOs should have is that they stand to lose market share by being undercut and being outpaced on technology by non-standard payments companies."

Others just feel that consumer protection, however, is an lurking undercurrent for an industry that is hustling to find innovative ways to stay competitive and turn an honest profit. "We are certainly living in the time of consumer protection," says Doug Varble, North American Vice President of Compass Plus, a technology development company serving the payment industry. Varble is located in their St. Louis, Missouri office. "Whether or not the financial industry meltdown was a result of consumer abuse, it has become the whipping boy and as such regulators will continue to try to "right" these perceived wrongs. Specifically, the CARD Act came about because of the immense profitability interchange fees were providing financial institutions. It can be expected that other profitability centers will be targeted in the same way."

For ISOs, there still are many challenges ahead.

"Several topics are coming to the fore in 2011, including resolving the issue of American magnetic stripe cards versus European 'chip and PIN' cards, particularly in the wake of the recent resolution by the European Payments Council requiring restricted 'use of magnetic stripe fallback' and permitting banks 'to refuse magnetic stripe transactions," says Donna Wilson. "In addition, a recent California Supreme Court decision, Pineda v. Williams-Sonoma, may chill efforts to engage in address verification for credit card transactions, for example, at the gas pump. The decision involved the interpretation of a California statute, the Song-Beverly Act, which generally prohibits merchants from obtaining personal identification information from consumers paying with a credit card at the point-of-sale, and recording that information. The Court held that zip codes constitute personal identification information under the Act, and the case has spawned literally dozens of putative class action suits. One of those suits, against numerous national gasoline retailers, accuses the retailers of unlawfully requesting zip codes as a condition of sale, and seeks up to the maximum statutory penalty of $1,000 per transaction.The plaintiff's counsel has described the case as potentially one of the largest class action suits in history, due to the number of credit card transactions at issue. Lastly, "hacktivism"—whether by insiders or outsiders at a company -- and as we've seen in the Wikileaks episode, is a clear and present danger in 2011 for credit card networks and systems."

But still, regulation has hit the industry in such a way that ISOs are just taking it below the belt. "Across the industry, the main concern right now is the cost of regulation," says Doug Varble. "With the CARD Act restricting the amount of interchange fees an ISO can charge, costs will be driven down so low that ISOs won't be able to make money servicing merchant accounts. They will loose the ability to make a profit and therefore lose interest in servicing merchant accounts. Merchants will have to go straight to their bank. ISOs must find ways to adjust their business model in order to make up for the interchange restrictions or loose significant market share.

Times like these may ripen opportunities to structure costs between merchants and ISOs. "It might be necessary to take a page from the banking handbook and shift the cost of regulation to other areas of the business or re-name costs," says Varble. "For example, a monthly or annual membership fee model could be implemented where merchants pay a flat amount opposed to a per-transaction cost. By at least offering merchants an option, ISOs have the potential of keeping some of them from switching to a bank as their processor."

But there is yet another dimension to regulation that is always part of the equation for all players in the industry: security and risk. "Cross-boarder fraud is out of control," opines Paul Kocher, president and chief scientist at Cryptography Research (CRI) in San Francisco, California. "The problem is going to quickly worsen unless card associations and issuers do a better job coordinating on international fraud issues. The United States' failure to adopt EMV is exacerbating the problem, since skimmed United States cards can be used internationally, and similarly magnetic stripes from international chip cards can be used fraudulently in the United States."

Kocher believes that the United States is at a crossroads between going contactless and adopting EMV. "The big danger is that the debate will delay the transition away from magnetic stripe. Every dollar of fraud, and every day that magnetic stripe remains dominant, the criminals are getting stronger, more numerous and wealthier." he adds. "Thus, by far the top security issue in the United States is to move beyond magnetic stripe. Significant fraud problems are brewing in the mobile space," he says. "Currently, malware on a handset today can't easily steal money, which helps limit mobile malware. The app store model encourages malware by driving software prices to zero and allowing unknown developers to get their software deployed, which creates opportunities for malware to get onto handsets. If phone architectures aren't built properly, for example if handsets end up with weaker security requirements than today's cheap EMV smart cards, mobile fraud is going to become a massive problem."

Gary Glover, Director of Security Assessment, SecurityMetrics, Orem, Utah can't emphasize enough how the collection of card transaction data using a mobile platform will be the talk of the town in the year ahead.

"I see huge pressure to leverage existing hardware in the form of smart phones, PDA's, etc. to run software that can process

manual or card present transactions," he says. "Processors are fast, apps are easy to write and most every device has a connection to the Internet in some way whether it be cellular, 3G, or wireless-based. Almost anybody can create a simple, attractive application to take card transactions and the barrier to entry is much lower than a vendor creating a dedicated hardware payment terminal. The security issues with these devices are that they are almost always connected directly to the Internet cloud and there isn't a firewall protecting access to these devices from hackers. In addition, the operating systems may not have been hardened against external attack, and there are many other types of insecure applications and communication running on the same platform the payment transactions are processed on such as texting and gaming. In other payment application environments the PA-DSS requirements help level the playing field and provide ways to certify a payment application is secure. Since the use of mobile platforms has grown quickly, the PA-DSS needs to be modified to address the unique security issues posed by this new application environment. The PCI-SSC is working feverishly to develop security guidelines for these mobile platforms during 2011 but until that time there is really no way to validate the security of payment applications running on these mobile platforms. I have a feeling that the payment industry will forge ahead using these mobile applications because they are so attractive. This does cause a security risk and may result in unexpected data loss situations until proper validation requirements are put in place."

Looking ahead, there are many things facing the ISO marketplace and the servicing of merchant accounts nowadays. According to Kocher, one of the biggest upcoming challenges will be the proliferation of payment instruments and systems. For example, network operators, financial institutions, platform vendors and handset makers all have conflicting aspirations to control mobile payments. "The result being a chaotic mix of incompatible technologies, protocols, rules, security policies, form factors and merchant experiences. ISO/MSPs will be caught up in the middle of all of this," he says.

"Over the next three to five years, I expect that we will no longer physically carry cards. As comfortable as we have become with our lives being stored on our phones, everything will be loaded onto our mobile device via an app and that will become our method of payment," says Doug Varble. "Significant planning will have to go into the creation of security standards, but the U.S. fraud rates will not decrease as long as we continue to physically hand our card to a person. In addition, an infrastructure will need to be developed that will enable the app to communicate with existing POS devices."

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.
Visit his website at www.JimRomeo.net.

back to articles