Visa Seeks New Ways to Keep Data Secret

By Eric Dash
Aug. 25, 2005

Inside Visa's operations center is a cool, white room about the size of a football field. There, more than a thousand giant computers, set up like hulking linemen, process cardholder information from across the United States.

The servers hum with some 3,000 credit and debit card transactions swiped through its network every second; they will handle more than 35 billion transactions in the next year.

Visa International is so protective of its American data center that visitors are allowed to say of the location only that it is somewhere in the central region of the United States. All the secrecy and cutting-edge technologies were set up to protect Visa's basic business interests -- encouraging credit card purchases and shielding banks from losses resulting from fraud.

As a result, nearly two months after the disclosure that a tiny payment processor, CardSystems Solutions, exposed the personal information of more than 40 million cardholders -- and even though Visa subsequently banned CardSystems from connecting to its operation -- the system remains as vulnerable as ever. Only now, with their brands at stake, have Visa, MasterCard and the other major card companies begun to focus on their consumers' main interests -- ensuring that personal information is secure at all times.

"These are akin to terrorist attacks; we must take very aggressive steps," John Philip Coghlan, the chief executive of Visa USA, said in an interview last month as he took over the card company's largest division. "We can sit here and say we have zero liability and that no consumer will be harmed. If trust is eroded, the very foundation of the system will be eroded."

Visa, like the other major credit card companies, has managed to reduce financial losses stemming from fraud, but it continues to struggle with preventing the theft of card data in the first place. Indeed, policing the payment chain is a herculean task, because virtually every step is outsourced from the time a card is swiped to the time the monthly statement arrives.

On any given day, data about Visa cardholders courses through the computer networks of

more than five million merchants, hundreds of data processors and 14,000 banks before it even reaches the machines at the Visa operations center. For online purchases, cardholder information can make additional pit stops at any one of the thousands of processing hubs in between.

Visa is responsible for ensuring that all the big retailers, data processors and banks that directly hook into its network meet its security requirements. But it is the job of the member banks to make sure that the merchants and data processors they hire follow Visa's rules. That leaves Visa, with a staff of 150 fraud fighters, to manage the security of an information pipeline that can leak at any time.

"There is definitely an implied responsibility from the merchant to the consumer, from the bank to the merchant and the card company for the oversight of the whole payment issue," said Robert J. McCullen, the chief executive of AmbironTrustWave, a Chicago firm that audits the security of card processing systems. "But accountability is much harder."

One reason is that Visa and MasterCard do not directly issue credit cards or sign up merchants. They are associations, marketing machines and policy makers that operate for the benefit of thousands of member banks, ranging from small credit unions to large institutions like Bank of America, J.P. Morgan Chase and Wells Fargo. They all pay association fees every time their merchant is paid or their customer's card is swiped.

Although Visa and MasterCard set the rules for their member banks and the data processors and merchants they contract with, enforcing those rules is complicated. The card companies, which in theory can fine or suspend banks, have little incentive to punish them because that would reduce the volume of transactions and cut into their fees.

Banks also have good reasons to look the other way when their merchants or processors do not comply. "They are required to publish the rules and enforce the rules, but at the end of the day, it's a game of chicken," Mr. McCullen said. "If your largest merchant says 'I'm not going to do it,' the odds of that bank pulling the plug are slim. They can always find another bank that will take that business."

Moreover, merchant advocates say the banks even profit from frauds if the losses are not too large. Not only do they take in charge-back fees from merchants of $25 to $30 for each fraudulent purchase, but in many cases -- especially those involving online merchants that have riskier transactions -- the retailer must also swallow the cost of the item purchased.

Security compliance is further hampered by a patchwork of data protection laws and regulatory agencies, each with limited mandates. There is no federal law or agency

requiring merchants to protect cardholders' data, though the Federal Trade Commission has recently shoehorned privacy violations into cases focused on deceptive practices.

Payment processors that handle millions of cardholder records are subject to ad hoc data security exams. But in most cases, only after a major data breach occurs do federal banking regulators investigate.

"Through outsourcing, they can essentially avoid responsibility for safeguarding consumer information," said Robert D. Manning, author of "Credit Card Nation" and a longtime critic of the payments industry. "Visa and MasterCard are membership associations -- and they have essentially failed in safeguarding the interests of consumers because they simply exist as an organization to protect the interest of their member banks."

"They are supposed to be ostracized, penalized, suspended, put on probation, whatever," Mr. Manning added, referring to the banks, data processors and merchants that fail to adhere to Visa's security rules. "It never happens."

Visa executives have strongly denied those allegations. But with the exception of CardSystems, which Visa has thrown out of its network effective in October, they have never produced other examples of banned companies, citing confidentiality concerns. And they are quick to claim that they are winning the war against bogus transactions. Today, the amount of money lost to fraud has fallen to about 5 cents for every $100 that is charged, compared with 15 cents for every $100 in 1992, according to The Nilson Report, a credit card industry newsletter.

The cat-and-mouse game with fraudsters is one that Visa and the rest of the payments industry have been playing for a long time, said Lewis Mandell, a credit card historian and professor at the State University of New York at Buffalo. "It was a price that one had to pay to get cards in the hands of large numbers of people," he said.

But the growth of the Internet and online retailers in the late 1990's resulted in larger and more sophisticated fraud schemes that forced Visa to step up its scrutiny. Now, computer-savvy criminals can steal thousands of card numbers from vulnerable databases and then collect a windfall by making small bogus purchases for a few dollars each.

"Here at Visa, we started talking about how do you start securing data in an environment where we didn't have much control over merchants and third parties," said John Shaughnessy, a Visa senior vice president for fraud risk. "We always had rules in place that said merchants and third parties had to secure data but we never said how to do it."

As a result, Visa drafted new security rules and required all its merchants and processors

to follow them by 2001. Big retailers like Wal-Mart and large processors like First Data Corporation were subject to audits certifying that they met standards like encrypting their data and passing quarterly vulnerability scans. Smaller merchants and processors with a substantial online presence had to meet slightly less stringent requirements. Visa's member banks, meanwhile, were told that they were responsible for compliance.

In 2003, Visa led a series of discussions with MasterCard, American Express and other major card brands to establish a set of security standards and a timetable for complying with them. Yet only one-third of the 400 small and midsize processors, which together handle about 10 percent of all domestic transactions, can say they currently meet the industry's requirements, even though the standards took effect in September 2004. Less than 0.3 percent of the country's roughly five million merchants are known to have taken any compliance steps at all.

"Just because you have the controls and rules doesn't mean you flip a switch and everything happens at once," Mr. Shaughnessy said.

Visa recently started holding seminars to educate small merchants and processors about its data protection policies. It has spent millions of dollars to develop sophisticated technology like Advanced Authorization, which can detect fraud at the time a card is swiped.

And in a highly unusual public move, Visa said it would not allow CardSystems Solutions to connect to its system; MasterCard has permitted the processor to continue, with upgrades to its security policies and equipment. The decision, after other high-profile data security breaches, has sent shockwaves through the industry, especially among processors and member banks.

Mr. Coghlan said that Visa could not do it alone. "The responsibility is really shared," he said. "We must work together to understand the weak points in our system, and understand that attacks and threats go to the very trust consumers have in these brands."

Of course, there may be another reason for the card companies to ensure their payment system is safe. "To the extent the payment industry doesn't police itself, the federal government and F.T.C. will do it for them," Mr. McCullen said. "If they step in, they are protecting the consumer -- not the payment industry."

A version of this article appears in print on , Section C, Page 1 of the National edition with the headline: A Matter Of (Fading) Trust; Banishing One Payment Processor Was Just the Start for Visa