Visa, Everywhere You Want to Be

Jim Tiller

Fraud is the bane of the financial industry’s existence. Financial institutions are constantly battling forgery, impersonation, and outright theft, and the advent of computers and the Internet, while increasing capability and efficiency, has exacerbated the problem. Visa has stepped in and started an information security program that seeks to revolutionize the industry.

Today, average people are continually fooled into providing confidential and private information by phishers who in turn steal their money and identities. Companies that process financial transactions are everywhere and are collecting vast amounts of your information. Many of these organizations are the target of crime syndicates and hackers seeking to obtain personal information to commit fraud.

Given the growing number of transactions, along with the number of merchants and providers processing credit card information, the implications of insecurity have the potential to move well beyond what we are seeing today. One could argue that if the risk of using one’s credit card continues to increase, it could adversely affect the spending practices of the public. This is especially true for burgeoning markets, such as China, India, Saudi Arabia, Kuwait, Oman, Qatar, and the United Arab Emirates, where credit card transactions are increasing in number and for discretionary spending.

Every country, established or emerging, wants to move away from cash transactions. Cash is expensive to produce and refresh, prone to counterfeit, and offers the means to launder illicit activities. In an attempt to counter credit card fraud, some organizations, such as American Express, implemented integrated circuits (IC) into the credit cards. They incorporated programmable logic in an effort to instill integrity in the transaction. At one point, American Express was offering USB card readers for online transactions. Unfortunately, average consumers were disinterested because they could not fully appreciate the risk from which they were being protected. Other organizations, more so in the United Kingdom, Germany, Switzerland, and France, could take advantage of smart-card technology in point of sale (POS) systems, arguably because of their pragmatic approach to security and a manageable geography. However, they too suffer from adoption, and aside from the IC, the credit card has changed very little in the last several decades.

An intriguing initiative (once again, started by American Express) was the provisioning of temporary virtual credit cards; specifically, virtual numbers. The process was simple: a credit card holder would access a Web site, authenticated and presumably secure, and acquire a virtual number that could be used on the Internet. The
limit of time and credit, along with semi-isolation of the cardholder’s private information, provided American Express, as well as the cardholder, a window of fraud protection in the face of countless vulnerabilities and threats associated with the Internet. Unfortunately, adoption of this new strategy waned and the process was ultimately decommissioned, to my chagrin as a consummate user of the technology.

So what are we to do? Threats are ramped, users are understandably detached, and if the problem continues, companies and countries risk poisoning their economic growth. The answer is to bypass the users and target organizations processing transactions, and this is exactly what Visa is doing.

In June of 2001, Visa introduced the Cardholder Information Security Program (CISP) to protect private constituent information where it resided in the credit system. The program established a collection of security requirements for merchants and services providers to ensure the level of security practices were reflective of the information they managed. This represented an enormous departure from traditional corporate tactics regarding security. However, to ensure merchants and service providers were meeting the requirements, Visa established a list of approved vendors — professional services providers (e.g., consultancies) — to perform audits.

In the beginning, the approved vendors simply had to demonstrate they were capable of performing an audit. Typically, they proved this by performing an audit and having the results reviewed by Visa. Regrettably, the approval process did not reflect the level of trust implied and results could not be substantiated, nor were their enough resources for Visa to audit the auditors. As with many before them, Visa learned a lesson: security professionals came to understand long ago: if there is no process governance, there can be no trust, and trust is paramount. Meanwhile, the increasing rate of fraud and identity theft, and all the byproducts of such activity, placed a great deal of pressure on the industry to reevaluate its approach.

Soon, American Express, MasterCard, and Discover began to take notice of Visa’s program. In fact, during the evolution at Visa, Master Card established a similar process focused on vulnerability analysis of Internet facing systems that process or store credit card holder information. It did not take long for these two giants to join forces.

In early 2005, Visa created a new process for approving auditors, and now other credit card companies are buying into it, representing a massive shift toward security and comprehensive governance in the industry never seen before. Upon deeper inspection, one has to appreciate Visa’s new process — its simple elegance and clear commitment to security.

First and foremost, the process of becoming a Qualified Data Security Company (QDSC) is not cheap. When all is said and done, it will cost a company roughly $25,000 to get started and average $15,000 per year, depending on various attributes. This cost demonstrates a company’s sense of commitment and investment in the process. Of course, for the likes of IBM, PWC, EDS, and other giants of the consulting industry, this is a rounding error. But for other companies emerging as security providers, and there are many these days, this is a noticeable expense.

Beyond the money there is the construct of the qualification process. A company wishing to become a QDSC must document and demonstrate its validity as a business, providing evidence such as business license, proof of insurance that meets Visa’s requirements, resumes and backgrounds of executive staff, legal posture, and hiring practices and policies.

Then comes the security capability. The organization must describe its security capability, experience, organizational structure, methodologies, and the time and resources spent performing security services. Of course, this is compiled by articulating what skills and experience the security practice has in the payment card industry. Visa validates this
information by requesting customer references to interrogate regarding their experiences with the applicant company.

Interestingly, and this is where Visa did it right, each consultant that is to perform Visa audits must meet stringent requirements. Each individual must provide a resume that includes years of experience, education, description of skills, work history with the company, and experience with the payment card industry. Additionally, candidates must have a CISSP, CISA, or CISM certification. However, this is where Visa gives a little bit. If a consultant does not have one of these certifications, they can document the last eight years of security experience. Applicants who can meet these requirements may be accepted to attend a security training class. Those who pass the test receive the Qualified Data Security Professional (QDSP) certification.

This is brilliant on Visa’s part. They are combining key attributes of the business, the company, and its resources to build layers of confidence in the provider beyond the legal agreements. In fact, an example of Visa’s focus is its requirement to prove it is in fact sending identified resources to the training before the company-level application is accepted. Moreover, if Visa does not like the company’s hiring policies and background check process, it retains the right to perform its own background checks on the QDSPs.

If a company meets all these requirements and manages to be accepted by Visa, then it must meet the core requirement of all this activity — performing audits. The company must demonstrate its quality control process to ensure a merchant or services provider — a customer of the professional services company — receives a deliverable that meets Visa’s standards and is free of errors. The deliverable comes in two types: a report on compliance (ROC) and a summary of findings (SOF). These must be reviewed for accuracy, completeness, and adherence to Visa’s standard before being signed by the QDSP and a representative from the QDSC.

Visa adds to the delivery requirements by demanding information about how the company protects its information. This may seem obvious to many, but in my experience there has always been a gap in how companies interpret the security of security companies. It would be confusing for Visa to approve a vendor to perform audits on how companies protect private cardholder information without requiring the same from the professional services vendor. This is another example of Visa’s thoroughness. Finally, Visa wants someone at the company with whom to interface, so primary and secondary contacts are required and must offer a process for secure communications, such as a PGP key.

Visa’s competence in demanding perfection is further demonstrated by the fact that each QDSP must be recertified every year. Moreover, there is a fee of $10,000 every year to maintain the QDSC status, and CISP audit customers of the QDSC must complete a quality review form expressing their experience with the QDSC. This closes the loop between process and governance.

A couple points are worth noting about Visa’s process that make it effective. The fact that a company, as well as its consultants, must be qualified brings organization to the entire audit process and governance. For example, if Visa were to simply offer an individual certification, there would be much less trust in the framework.

Another attribute I appreciate is the interrogation of the quality control and security practices of the company. As stated earlier, this should be expected, but companies rarely enforce this at the level Visa has.

Finally, the maintenance and administrative aspects of the certification of individuals and the company cannot be understated. Too many companies slip under the ethical and competence radar in providing security services.

Visa has taken a program with good intentions weakened by lack of meaningful governance and completely reorganized it around a process that is pragmatic, yet highly effective. The good news for all of us
is Visa has initiated a trend that will consume the financial industry. MasterCard has already expressed it will utilize the same framework established by Visa for its merchants and service providers, and American Express and Discover are joining the march.

It is important to fully understand what is happening here. This isn’t another government regulation that is open to interpretation and blind to unique company challenges. This isn’t another security standard that organizations adopt in their own way. And this isn’t a halfhearted attempt to address a global issue. This is economic governance at its best, and Visa has put its reputation and the company’s success on the front line of information security. For example, when a merchant or service provider does not meet the security requirements and fails to address them, it is expelled from the system! This means Visa will not receive revenue from that company’s credit card transactions. On the surface, one would assume that the merchant simply ignores Visa and offers customers American Express, Discover, or some other credit card payment method. However, because other companies are joining Visa’s endeavor because they know this to be the right thing to do for the industry, the merchant may quickly find itself unable to receive payment from customers wishing to use credit instead of cash.

In my humble opinion, this is huge. Yes, of course this does not solve all of our security problems; identities will still be stolen, fraud will still be committed, and hackers will continue to steal credit card numbers. But this is a positive development that will have a measurable impact on the industry for years to come. And most important, it sets a precedence that other industries can follow and use as a foundation that can be modified and improved upon to address the specific challenges they face in a digital world.

So, if you’re a merchant or service provider, expect some security focus coming your way. And if you’re a credit card holder, you may find a little more comfort in knowing that there are companies out there that are trying new things to address new problems.