

Data breaches happen; we're all trying to get over it

It was and continues to be big news, starting a couple weeks ago: Global Payments Inc. reported unauthorized access to its processing system affecting credit card payments. On March 30, the company said less than 1.5 million card numbers may have been exported.

That sounds really bad, and it is. Visa rightly removed Global Payments from its Payment Card Industry compliance list. (PCI is a data security standard managed by the PCI Security Standards Council.)

To its credit, though, Global Payments has endeavored not only to work to repair the damage but to let everybody know what it is doing. On April 1 it laid out what it's determined so far: The breach was confined to North America; only Track 2 card data may have been stolen, meaning cardholder names, addresses, and social security numbers were not compromised; and forensic analysis, network monitoring, and additional security measures indicate the incident is believed to have been contained.

Global Payments quickly set up a dedicated website to answer questions from cardholders and merchants, as well as others, as to what this means. It's quite apparent what the main message the company wants to impart, as it repeats it in several places on the site: "This incident will not adversely affect merchants or their relationship with their customers."

It's what any company would do for damage control, but it is something. Zilvinas Bareisis, an analyst at Celent, wrote in his blog as he reported on Global Payments, "As the commerce environment gets more complex (online, offline, mobile, etc.) and as access points to payments proliferate, security issues are only getting more complex."

A lot of people are deeply involved in the bigger issue of the intersection of commerce and security technology. Buying things and services through various tech gizmos will only increase; and making those transactions secure will only become more imperative.

IBM has a security unit—the IBM X-Force—whose members must have the coolest t-shirts. This group of techno-analyst-geniuses recently issued its annual report regarding the security trends and risks it found in the past year. It has some promising news, and some troubling news.

On the plus side it found:

- A 50% decline in spam email compared with 2010.

- More diligent patching of security vulnerabilities by software vendors, with only 36% remaining unpatched in 2011,

compared with 43% in 2010.

- A higher quality of software application code, as seen in web application vulnerabilities called "cross site scripting"; half as likely to exist in clients' software as they were four years ago.

On the dark side, however, the X-Force found: A rise in emerging attack trends including mobile exploits, automated password guessing, and a surge in phishing attacks, as well as an increase in automated shell command injection attacks against web servers.

"In 2011, we've seen surprisingly good progress in the fight against attacks through the IT industry's efforts to improve the quality of software," says Tom Cross, manager of Threat Intelligence and Strategy for IBM X-Force. (Now that's a cool title.) "In response, attackers continue to evolve their techniques to find new avenues into an organization. As long as attackers profit from cyber crime, organizations should remain diligent in prioritizing and addressing their vulnerabilities."

With the Global Payments incident, it's obvious the cybercrooks have continued to evolve their techniques. As long as they do, it's a sure bet the technology vendors will continue to evolve their defensive security products and services. Here's a list of vendor announcements just within the past month, all aimed in one way or another to thwart the cybercriminals:

- MasterCard introduced Expert Monitoring Fraud Scoring for Merchants, a tool that provides merchants with a predictive fraud score for card-not-present transactions in real time to measure the likelihood that a transaction is fraudulent.

- Visa offered a new service that provides financial institutions and mobile network operators with a one-stop solution to securely download payment account information to NFC-enabled smart phones.

- LexisNexis Risk Solutions launched enhancements to its TrueID fingerprint biometrics, adding: LexisNexis One Time Password, an authentication method for high-risk, high-value customer transactions; and LexisNexis Voice Biometrics, a speaker verification system.

- Kony Solutions allied with VASCO Data Security International Inc. to integrate their respective mobile application development platform with a strong user authentication solution.

- Trusted Logic Mobility partnered with Wave Systems Corp., to provide a solution that allows encrypted data held in a corporate laptop computer to interoperate securely with properly evaluated smart phones.

• The Shazam Network partnered with United Bankers’ Bank to offer the proprietary ID TheftSmart available to financial institutions in the network—financial institution customers who enroll in ID TheftSmart receive one-on-one access to licensed investigators with Kroll Inc., in case they become victims of identity theft. (This offers the additional benefit of being a revenue source for the financial institutions.)

Even as Global Payments struggles to recover from its security breach, and even as these vendors breathlessly explain the latest security protections, there really is no end in sight. New technologies such as mobile, social media, and cloud computing continue to create challenges for enterprise security.

As Celent’s Bareisis quoted Global Payment executives in what must have been a very painful teleconference, the company “intends to get its record of compliance back as soon as it is humanly possible, will spend even more on security going forward, and expects to come out stronger and more experienced as a result and believes that customers will recognize this.”

Sources used in this article include:

[Global Payments Provides Updated Information Regarding Unauthorized System Access](#)

[Some Facts About Data Breach at Global Payments](#)

[IBM X-Force Report: 2011 Shows Progress Against Security Threats But Attackers Adapt](#)

[MasterCard Introduces New Tool that Predicts the Potential for eCommerce Fraud in Real Time](#)

[New Visa Service Provides Secure Over the Air Provisioning of Mobile Payment Accounts](#)

[Kony and VASCO Form Alliance to Offer a Higher Level of Security for Mobile Applications](#)

[LexisNexis Launches Multi-factor Authentication Solutions to Help Mitigate Identity Theft and Fraud](#)

[SHAZAM Launches Consumer Identity Theft Protection](#)

Trusted Logic Mobility and Wave Present Joint Security Solution for PCs and Mobile Devices

About the Author

John Ginovsky is contributing editor of ABA Banking Journal and editor of the publication's TechTopics e-newsletter. For more than two decades he has written about the commercial banking industry. In particular, he's specialized in the technological side of banking and how it relates to the actual business of banking. He previously was senior editor for Community Banker magazine (which merged with ABA Banking Journal) and was a staff writer for ABA's Bankers News. You can email him at jginovsky@sbpub.com