



2009 Global Security Summit
SECURING THE FUTURE OF PAYMENTS



2009 Global Security Summit Summary Report



2009 Global Security Summit Summary

Event Overview:

On March 19, 2009, Visa Inc. hosted its third Global Security Summit, “Securing the Future of Payments,” presented in partnership with the Economist Intelligence Unit. The event brought together business, government, academic, and law enforcement officials to discuss how payment system participants can collaborate to protect cardholders against current and emerging security threats. Three keynote speakers and five panels were assembled to cover a range of topics, including innovations in payment security, e-commerce security, small business data protection, global security priorities and the growing sophistication of modern criminals. In the midst of a global economic crisis, participants from across industries and around the world illustrated the importance of aggressively securing the payment system.

Key Points:

- Despite recent high-profile breaches, the payment system remains secure. Fraud rates in the industry remain near all-time lows.
- There is no “silver bullet” to protect payments; security requires multiple layers of tools and approaches to ensure all avenues are protected.
- Good security is a shared responsibility, so collaboration is critical among all entities that handle data and protect consumers – issuers, acquirers, retailers, processors and law enforcement.
- The Payment Card Industry Data Security Standard (PCI DSS) remains an effective standard; it has had the single greatest impact on the security of the system and remains the best defense against the loss of sensitive data. However, challenges remain to ensure ongoing compliance.
- Fighting fraud remains an arms race against data thieves. Criminals are becoming increasingly sophisticated and they are relentless in trying to obtain consumer data. The economy is creating more desperate criminals and their efforts are being stepped up. Criminals are well-funded and well-organized, and even if they are caught, they often face only minimal punitive consequences from government authorities.
- Criminal fraud moves to find areas of vulnerability. Whether geographically, by business size, or via channel, when security is strengthened in one area, criminals move to find another vulnerable area to target.
- Offering workable security solutions for small businesses is critical. Many small businesses do not recognize their risk, and with limited resources, many may be hesitant to invest in more security, particularly in tough economic times. But the industry must work together to educate those businesses and offer them simple and affordable solutions.
- The industry needs to apply greater focus to devaluing cardholder data to render it worthless to criminals, including pursuing dynamic authentication solutions.
- Significant opportunity exists for a coordinated law enforcement effort to promote data security and consumer protection. Cyber crime is borderless and requires an international approach that is not always possible in emerging parts of the world. A holistic approach would help with both enforcement and punishment that fits the crime, regardless of where the criminal is located.
- Even in the face of economic challenges, the industry must maintain its commitment to investing in security.



Welcome Keynote Address

Visa, Inc.'s **Chief Enterprise Risk Officer Ellen Richey** welcomed Summit attendees with an address highlighting the real progress made in the fight against fraud, resulting in payment card data fraud rates that remain near historic lows despite economic woes and high-profile compromises. To continue that success, Richey called for continued industry investment, collaboration and innovation to keep the electronic payment system secure in the future.

Key Points:

- **Substantial progress has been made since the 2007 Visa Security Summit.** First, corporate leadership has risen to the challenge of making security a strategic priority. In fact, in a recent Economist Intelligence Unit poll of global executives, 75 percent said a C-level executive is now responsible for payment security within their company. Second, massive investments and innovative solutions have helped keep fraud rates in the industry near all-time lows. Third, real progress has been made in expanding adoption of the PCI DSS, with 90% of large U.S. merchants now validating compliance. Fourth and finally, Washington is focusing on this issue, with President Obama creating a National Cyber Advisor post, committed to increasing focus on cyber crimes, in partnership with industry.
- **Economic pressures make it critical to focus on security, despite budget constraints.** Mitigating fraud is an arms race against data thieves. Despite great strides in the reduction of stored data, criminals are aggressively targeting data in transmission and large-scale environments. The economic crisis has raised levels of desperation and opportunity, making it critical that the industry redouble its efforts as educators and advocates for data security. Years of progress in building consumer trust could be eroded if the industry is not more efficient, more vigilant and more convincing than ever in ensuring that critical investments in security continue to be made. It is the only way to assure businesses and consumers that they can trust the system to deliver value, safely and securely.
- **Securing the payments system requires a multi-layered approach — there is no “silver bullet” solution.** As criminals get more sophisticated, the industry must also get more creative in building multiple layers of security — in technological innovations, in partnerships, in business processes — to stay one step ahead. There are four approaches the industry can take to provide these multiple layers:
 1. **Actively manage the threat of compromises, and do so in a way that does not unnecessarily burden business.** The PCI DSS remains an effective security tool when implemented properly and it is the best defense against data theft available today. But those standards can only significantly reduce the risk of breach if they are fully implemented and consistently followed. PCI DSS is not meant to be exhaustive. The standards provide a strong foundation — and the best security strategies build on that foundation to create a multi-layered and evolving defense.
 2. **More actively engage consumers and empower them to help protect themselves.** According to a 2008 Javelin study, just over half of consumers view the responsibility for protecting financial accounts from fraud as equally shared between themselves and their financial provider. Everyone has a role to play in securing the system — including consumers themselves. And so, while Visa and its issuers already monitor and risk-score transactions, even more can be achieved by providing consumers with additional tools and putting more information in their hands. Visa recently announced a transaction alerts and notifications service, currently available to Chase cardholders with Android mobile devices, and coming later this year to all Visa issuers. Visa is also developing a targeted acceptance service allowing consumers to set personal limits on how their cards can be used — such as dollar amounts, geographic limits or merchant segments.
 3. **Increase collaboration across the payments system to close security gaps and share critical information faster.** Collaboration is critical to the industry's mutual success and nothing is more important than sharing information. In 2008, Visa launched Visa Risk Manager, as an intelligent



decisioning service for issuers. Visa is also increasing information sharing with merchants through a version of its Advanced Authorization risk scoring service, tailored for online merchants.

- 4. Continue to reduce the value of stolen data, through investment in new authentication measures.** The future lies in finding ways to make stolen data unusable, in particular through innovative authentication. There are differing needs, threats and infrastructures in different parts of the world, requiring different authentication means - there is no "one-size-fits-all" answer. Visa believes the best way to make data unusable is by introducing dynamic data into the transaction authentication process.



Panel I – Innovations in Payment Security

Data thieves are increasingly sophisticated in targeting card information — both stored and in-motion — and the impact touches all payment system stakeholders. The Innovation panel explored what the industry can do to reduce the storage of data, including compliance with the PCI DSS, but also how to make that data unusable to criminals through innovations in authentication and encryption.

Key Points:

- **Though there is no single solution to data fraud, there are many ways to prevent attacks.** At the card level, which is the first-line of defense, the industry can provide an added level of security with innovations like dynamic data cryptograms. At the terminal, technology and authentication can be enhanced at the actual point of sale. Through continued fraud monitoring, address verification, and launching Advanced Authorization services, the power of the Visa network provides the third approach to preventing attacks. Visa is working to find other solutions against three guiding principles: solve for all channels and all transactions; invest strategically against high-risk targets; move from static to dynamic data.
- **Security and convenience need to be balanced to preserve the customer experience.** OfficeMax is currently working with Visa on a pilot program to add an additional layer of verification at the point-of-sale. Conducted at 100 stores in Illinois, Indiana, and Florida, customers were asked for either their zip code; the last 4 digits of their home phone number; the last 4 digits of their cell number; or the 3 digit area of their home phone. The effort provided a targeted and dynamic way of addressing fraud. Overall, feedback indicated that the experience was good, with no noticeable impact for OfficeMax's customers.
- **It is important to develop ways to make data unusable.** While PCI DSS is an important defense, unrelenting efforts to find vulnerabilities continue to give hackers an advantage. If those hackers can access information, it is critical that that data is unusable. Encryption can be a useful solution, but there are significant key management issues that need to be considered. Fifth Third Bank engaged in a pilot program with Visa, called "Digital ID," installing 1,000 special readers across a number of different merchants as part of their normal upgrade process. The pilot leveraged the fact that the magnetic stripe of a card is physically unique, and can provide a fingerprint for that particular card. Upgraded terminals can detect the magnetic stripe's fingerprint, and Visa can verify if the card is genuine or counterfeit. No key management is required. The pilot program has worked well to date.
- **End-to-end encryption can also help make data unusable.** Spain developed a systemic solution for removing track data from the merchant environment, improving significantly the security of the whole payment system in that country. All acquirers in Spain worked together to introduce end-to-end encryption. The encryption key is stored at the merchant's acquirer, eliminating the need for the merchant to manage it. When the information is in transit or being stored in the merchant environment, it is ciphered completely, so if a hacker obtained any of the data, it would be unusable. When the transaction information reaches the acquirer environment, the data gets decrypted and then proceeds regularly through the payment system.
- **Network segmentation offers strong security and can help sell-in security efforts with other business propositions.** Segregating transaction information from other processing efforts at the point of sale can minimize risk and help implement security changes more easily. For McDonalds, where speedy transactions are critical, they do not store track data in their stores. Transaction data is managed outside of the store environment, and none of the internal systems can see the data. McDonalds is able to integrate this service and bundle it with other operational enhancements, helping franchisees better manage their data security investments.

Moderator: Avivah Litan, Distinguished Analyst, Gartner

Panelists:

- Gerry Sweeney, Global Head, eCommerce & Authentication, Product Innovation and Development, Visa, Inc.
- William Van Orman, Treasurer, OfficeMax, Inc.
- Don Roeber, Vice President, Fifth Third Bank
- Carmen Carnero-Silvo, Deputy Managing Director, ServiRed S.A./SERMEPA S.A., Spain
- Dave Weick, CIO, McDonalds Corp.



Keynote Address

Dave DeWalt, CEO and President of McAfee, informed attendees that now, more than ever, security is mission critical for all organizations. He called for cross-border collaboration and for businesses to make security a priority through assessing risk, closing gaps, and being vigilant.

Key Points:

- **What's happening in the cyber crime world is the exact opposite of what's happening in the economic world.** As the economy continues in crisis, criminals are stepping up their efforts to attack on all fronts. McAfee has recently seen a 500% increase in malware (malicious software), which is more in the past few months than in the past few years combined. That is reflected in a 22% increase in reports of ID theft victims, and a 40% increase in consumer complaints to the Federal Trade Commission. "Trojans" continue to be the most insidious, as they can load onto a computer and siphon off data. Already in 2009, 80% of Trojans were financially motivated. Trojans are emerging through expanding social networking technologies like Facebook, MySpace and LinkedIn. This expansion is helping to drive a now \$1 trillion economic problem related to lost or stolen intellectual property.
- **Dramatic increases in malware across the board highlight vulnerabilities.** The dramatic increase in malware is being seen across the entire technology ecosystem. That increase is only being helped by a substantial increase in smart, online devices that make it easier for them to spread - more applications; more technology; more memory. With all these devices comes a dramatic increase in data loss potential. The level of sophistication of these criminals is significant, while the risk to them remains very low. Regulations and compliance requirements may be expanding as well, but with a global network that is inconsistent from country to country, they do not always help the way they should.
- **With vigilance and collaboration, there are many approaches to addressing cyber crime.** In many instances of cyber crime, technology was available to address vulnerabilities, but had simply not been deployed. Companies should be sure to implement technology that is already on the market, like basic encryption of removable storage and data-loss prevention systems. Education of consumers and corporations is critical. Lastly, better legal frameworks are needed, with modernized cyber crime law that is consistent across emerging nations, so once criminals are arrested, they face punishment appropriate to the significance of the crime.



Panel II – Payment Security – the State of Global Readiness

Are global companies ready for the security challenges and opportunities presented by the increase in electronic payments? The Economist Intelligence Unit unveiled a new global study of the world's executives that explored how the C-Suite prioritized payment security and their level of preparedness. Executives from Russia, Singapore, Brazil, and Mexico discussed results of executive roundtables in each of their countries and provided perspectives on securing payments.

Key Points:

- **Globally, C-suite executives believe that data fraud is a growing threat that requires more collaboration among industries.** In October 2008, Visa and the Economist Intelligence Unit commissioned a survey about the future of payments industry, with a sample comprised of 60% from financial services and 40% from retailers. More than one-third of the survey respondents were from the C-suite, and roundtable discussions were held in Mexico, Brazil, Singapore and Russia. The survey found that respondents rated payment security as their second most important challenge – (their top challenge was efficiency). There was a significant split between executives who believe breaches are rising (50%) and those who believe breaches are stable (40%). Financial services respondents were more likely to say there was an increase in fraud than the retailers were, and 20% of all respondents said that criminals were more sophisticated. 60% say they believed their investments in security are in line with their risks of loss. Most respondents did believe that collaboration is the most effective way to improve security.
- **Fraud moves from place-to-place or channel-to-channel, as security increases and vulnerabilities develop elsewhere.** As authentication technologies like chip become more ubiquitous, fraud seems to be moving to card-not-present. The industry needs to be vigilant about what is going on in the market and where criminals are looking for opportunities. Such efforts will help guide strategic investments in different channels (e.g., mobile, internet, etc.).
- **Education is key, as it empowers consumers across the globe to protect themselves.** Making consumers aware of not only their risk, but what they can do about it, will help combat fraud and keep the system safe. One example – particularly effective in Brazil – is the use of SMS messages to inform consumers every time their card is used.
- **Emerging countries with differing mindsets and regulations continue to be a problem.** Overall, the industry needs to work together to secure a regulatory system that addresses the “no-boundary” nature of data fraud. Large discrepancies between different regions make prevention and enforcement efforts challenging. While consumers in Brazil may be familiar with dynamic authentication via tokens, in Russia, cash is still king, and consumers do not yet have the mindset for utilizing cards. Education in the less-sophisticated regions is particularly important, and in many cases, government can play a big role in educating the public if they are properly educated themselves.

Moderator: Nigel Holloway, North America Director for Industry and Management Research, the Economist Intelligence Unit

Panelists:

- Alvaro Teofilo, Superintendent, Security Operations Center, Prohuban-Grupo Santander, Brazil
- Gurinder Nihal, Country Head, Global Transaction Services, Royal Bank of Scotland, Russia
- Stephen Y.W. Chang, Executive Director and Head of Cards – Asia Pacific, Treasury Services, JPMorgan, Singapore
- Gaston Huerta, Director, Fraud Prevention, BBVA Bancomer, Mexico



Keynote Address

Martha Coakley, Massachusetts Attorney General, told attendees that privacy protection, safety and security are part of an ever-changing landscape as government, law enforcement, industry and consumers seek to balance technological advances in society with traditional expectations of privacy and security. The challenge is to seek collaboration and cooperation among all stakeholders to share knowledge, pool expertise and work in concert to ensure that consumers are protected.

Key Points:

- **Identity theft is a growing problem that affects both private and public sector stakeholders.** Unfortunately, more and more consumers are becoming victims of identity theft. Between January and December 2008, the Federal Trade Commission received more than 300,000 identity theft complaints – approximately a 26 percent increase. Consumers must have confidence in a company's ability to safeguard their personal and financial information. Loss of that confidence could easily translate into a loss of dollars for business.
- **The Attorney General has championed efforts to combat identity theft.** Creating and implementing strategies and solutions to combat identity theft will require thoughtful planning and commitment from decision makers in both the private and public sectors. As part of this effort, Massachusetts adopted identity theft legislation to safeguard the privacy of consumers' personal information. The consumer protections covered under this comprehensive identity theft law seek to minimize the incidences of identity theft by ensuring that organizations notify consumers if there has been any unauthorized use or access to the consumers' personal information, requiring organizations to better protect information to prevent future data breaches, and providing consumers enhanced safeguards to prevent identity thieves from opening credit in their name.
- **The Massachusetts approach is a comprehensive effort.** A written information security program should include policies that require designation of one or more employees to maintain the program, assessment of internal and external risks to the security of personal information, procedures for preventing terminated employees from accessing records, limitations on the collection and use of consumer data, and disciplinary measures for violations. The legislation also requires businesses to establish computer security system requirements such as encryption of personal data stored on laptops or portable devices or transmitted through wireless or public networks.
- **These measures should not unduly burden business.** The Attorney General's office is paying close attention to how these regulations affect the business community, especially as many businesses face current financial challenges. In light of these considerations, the compliance deadline has been extended from January 1, 2009 to January 1, 2010 to provide some flexibility to businesses working to implement these measures.



PANEL III – Small Business – The New Target of Data Thieves

Criminals have always preyed upon the weakest link, and now some have set their sights on small businesses. Small businesses represent an increasingly larger percentage of compromise incidents yet are the least prepared to deal with such challenges to their business. This panel explored the emerging trend of small business as targets and discussed what must be done to combat the growing problem.

Key Points:

- **As larger companies bulk up security efforts, fraudsters turn to attacking smaller companies.** High-profile breaches make everyone in the business community more aware of the risk of data fraud. But small businesses are becoming more and more vulnerable to breaches as larger companies, with tightened security, are increasingly more difficult targets for criminals. But in these difficult economic times, more and more small businesses that need to increase sales are turning to the internet, without adequately addressing the increased risk to their data. In general, smaller companies do not always recognize the significance of their risk. In a survey of small businesses, more than half of all small businesses reported experiencing a security breach, but nearly one-fifth do not use virus-scanning software, and nearly 60% do not protect their wireless network with encryption. These findings reflect the reality that small businesses tend to act reactively to data breaches, purchasing protection only after suffering a loss. These businesses need to be educated on their risk and how to find the balance between actively managing the threat of a compromise, without placing an undue burden on themselves.
- **Ongoing compliance with PCI DSS is particularly challenging for small businesses.** The PCI DSS standards are valuable and important, but for small businesses, they are complex and expensive. Since many small businesses do not have the resources to focus on meeting compliance, affordable solutions should be considered, such as outsourcing to PCI DSS compliant service providers. Barclaycard, working with Visa Europe, has tried to extend the progress that has been made to secure the physical point of sale to the e-commerce world. As small business owners try to increase sales through opening an online channel, some find that they do not have the expertise to ensure e-commerce payment security. Visa Europe now has 20-22 secure and compliant payment pages that are available for any small merchant to use within their e-commerce environment.
- **As resources dry up in tough economic times, public and private sectors must work together to assist small businesses.** Visa Canada worked with the Canadian Chamber of Commerce on a report to help the Canadian small business community better understand the state of their fraud protection. Ninety-three percent of small businesses responded that they use virus protection, but 19% have no secure server, and 43% are not backing up their information. Two out of three thought security breaches were just happening to big business, while actually 85% of data fraud is happening to small businesses. Overall, the learnings demonstrated that small businesses needed solutions, but they must be easy to use and easy to explain. With the importance of e-commerce to the small business community, the Chamber of Commerce in Canada recommended the public and private sector work together by establishing a national panel and focusing on the importance of e-commerce security.

Moderator: Steve Salter, Vice President, BBBOnline

Panelists:

- Dr. Charles Matthews, President International Council for Small Business
- Merrill Phelan, Manager, Information Systems & Programming, Washington Metropolitan Airport Authority
- Chris Gray, Director, Canadian Chamber of Commerce
- Paul Cook, Managing Director Barclaycard Payment Acceptance, & Board Director, Barclaycard, U.K.



PANEL IV – E-commerce

Card-not-present fraud is a growing global problem for all payment participants, but fighting it requires a layering of different local market strategies. The E-commerce panel examined the unique and ongoing challenges of conducting commerce in a faceless, cardless environment and the new risk-based techniques, policies and processes that the public and private sectors are exploring to ensure the continued growth of global e-commerce.

Key Points:

- **All participants in the payments system need to build in security.** PCI DSS has had the single greatest impact on the industry, specifically by setting an expectation that security is as critical as safety belts are — it needs to be built into the system and should not be considered an option.
- **E-commerce security will require a solution for authentication in a cardholder/card-not-present environment.** When neither the cardholder nor the card are present, confirming the user's identity and authenticating the transaction is a particular challenge, and criminals are exploiting that to commit fraud. Government can take a significant role in reshaping that environment by helping strengthen tools for identity assertion, such as issuing the online equivalent of a driver's license.
- **New technologies can assist with securing e-commerce, but they often face their own challenges.** As technologies are rolled out, consumer behavior can sometimes cause more hurdles than technology. For example, Pay by Touch was never embraced because the sign-up process was too laborious for the consumer. Education can be effective in overcoming these hurdles, but technologies need to be better integrated into product development to address user adoption.
- **More severe penalties for cyber criminals needed.** E-commerce has created a jurisdictional nightmare for law enforcement. But because of the inter-connected nature of e-commerce, Criminals can penetrate vulnerable areas to reach better secured systems, since the internet connects them all. Unfortunately, while these are serious crimes, criminal law has not yet gotten up to speed, and fraudsters seem to only receive a "slap on the wrist." Law enforcement must "shrink the sanctuary," so that if penalties are increased, criminals living in certain countries can be prosecuted.

Moderator: Dave Hogan, SVP and CIO,
National Retail Foundation

Panelists:

- Orson Swindle, Sr. Policy Advisor,
Centre for Information Policy
Leadership
- James Andrew Lewis, Center for
Strategic and International Studies
- Mauricio Icaza, Director of operations,
Bradesco Cards, Brazil
- Heather Gorringer, Owner,
Wigglywiggles.com, UK
- Kristin Lovejoy, Director IBM Corporate
Security



PANEL V – Meet the Experts on Cyber Crime and Computer Intrusions

To solve a problem, one must first understand it. This panel was made up of cybercrime experts — from a former data hacker to a law enforcement agent who tracks criminals. These cyber crime professionals provided a rare glimpse into the mind and motives of today's data thieves. The panel explored hacker techniques and the ongoing race for law enforcement and the industry to keep pace.

Key Points:

- **Criminals are getting more aggressive and smarter.** Hacking used to be done by hobbyists, but now international criminal syndicates are the ones targeting cyber victims. They are well-educated professionals who engage in crime and who, through their networks, currently hold the advantage. The hacking community uses every possible opportunity to share their data, while the industry does not. While criminals become smarter and more aggressive, lawmakers and even the general public do not recognize or acknowledge the serious risk these criminals' activities pose. A recent Center for Strategic and International Studies report discovered that the majority of Congressional leadership does not realize the seriousness of the problem. Without increased knowledge and recognition by decision-makers around the world, efforts to combat cyber crime could be seriously hindered.
- **Criminals are able to engage in these acts with very little consequence.** Cyber crime is a global problem with lots of untouchable criminals, because they often reside in countries with little or no law enforcement. This has caused a fundamental shift in law enforcement. Law enforcement used to be local, based upon geography, but the concept of jurisdiction is basically dead when it comes to cyber crime. Law enforcement efforts must rely heavily on international efforts, but enforcement against border-less crime is often subject to serious deficiencies in developing countries. And even when criminals are caught, the current penalties on the books are not enough to lead to deterrence.
- **PCI DSS is an important defense, though not the single answer.** PCI DSS is an excellent framework. It is not the answer to every challenge, but it has significantly raised awareness of security principles. However, there are businesses that approach compliance as a periodic assessment. It is important to continue the life cycle on an on-going basis, exercising vigilance and maintaining compliance over time.
- **There are a number of approaches the industry can take to combat criminal efforts.** Despite the sophisticated nature of these crimes, stopping the criminals often still comes down to old-fashioned police work. For example, the arrests in the TJX case were the result of undercover agents working around the globe, infiltrating criminal networks. Technologies continue to provide the greatest opportunities with increasing refinements and innovations. Authentication features protect data quite well, but their features should be default, rather than discretionary. Increased cloud computing technologies currently in development may provide an opportunity to "reboot" security efforts. In addition to high-technology solutions, the industry should also look at staffing and employee training. Often some of the lowest-paid individuals in a company are responsible for the IT systems, exposing companies and making them vulnerable to data loss.

Moderator: Joe Majka, Global Head of Fraud Control and Investigations, Visa, Inc.

Panelists:

- Kevin Mitnick, Consultant, Mitnick Consulting
- Dan Kaminsky, Director of Penetration Testing, IOActive
- Mark Grantz, Special Agent, U.S. Secret Service
- John Stewart, Vice President and Chief Security Officer, Cisco Systems, Inc.