**Prepared testimony of**
**W. Joseph Majka**
**Head of Fraud Control and Investigations**
**Visa Inc.**

**Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology**
**of the**
**House Committee on Homeland Security**

**“Do the Payment Card Industry Standards Reduce Cybercrime?”**

**311 Rayburn House Office Building**
**Tuesday, March 31, 2009**

**Introduction**

My name is Joe Majka. I am the Head of Fraud Control and Investigations for Visa Inc. I have been with Visa for over 12 years and have over 28 years of experience in corporate security, investigations and law enforcement, specializing in the area of financial crimes. I want to thank the committee for this opportunity to appear at today's hearing and explain who Visa is and our role as a leader in global data security. Visa plays a unique role in the financial system, facilitating commerce among millions of consumers and businesses here and around the globe. It is important to note that Visa's fundamental role is to facilitate transactions between consumers and businesses. Visa is not a bank. We do not issue payment cards (credit, debit or prepaid), make loans to consumers, or set the interest rates or fees associated with card usage or acceptance. Visa is a network that serves as the connection point between 1.6 billion global payments cards, 29 million worldwide merchants, and 16,600 financial institutions in 170 countries. In making these connections, Visa helps create significant value for each of the participants in our system. Consumers receive a more convenient, secure and widely accepted way to make payments. Retailers benefit from the speed, efficiency, security and reliability that only electronic payments can provide. They also receive guaranteed payment and can avoid the need to extend credit directly to their own customers. In fact, the entire economy benefits from electronic payments through more transparent, secure and cost-effective commercial activity. The Visa Payment System plays a pivotal role in advancing new payment products and technologies, including initiatives for protecting cardholder information and preventing fraud.

We're pleased to be here to talk with you about data security in the payment card industry and about the Payment Card Industry Data Security Standard in particular. But, I want to put this discussion in the context of a multi-layered approach to security that includes fraud control measures from the card, to the terminal, through to the Visa network. Visa understands that we must protect each link within our control and work with others to preserve the trust in every Visa payment. Visa is keenly focused on ensuring that payment products are not used to perpetrate identity theft or other criminal activity. Our goal is to protect consumers, merchants and our client financial institutions from fraud by preventing fraud from occurring in the first place. To that end, Visa employs multiple layers of security, of which the PCI standard is an important one, but only one of many. We have taken a leading role in promoting cardholder information security within the payments industry. Visa and our participating financial institutions also provide solutions to prevent fraud and protect cardholders in the event of a data compromise. These include real-time fraud monitoring, identity theft assistance, consumer alerts, and zero liability for cardholders on fraudulent transactions. Visa provides sophisticated neural networks that enable our client financial institutions to block authorization transactions where fraud is suspected. Thanks to massive investments and innovative solutions, compromise events rarely result in actual fraud and fraud rates in the payments industry remain near all-time lows.

The payment card industry, regulatory agencies and law enforcement have individually and collectively taken extensive measures to prevent and mitigate the effects of consumer information compromises. In this regard, Visa has required all entities that store, transmit or process Visa card data to comply with PCI DSS standards, has implemented incentives to encourage payment participants to make the significant investments needed to attain compliance, and has taken numerous steps to minimize the amount of cardholder data stored by system participants.

**Payment Card Industry Data Security Standard**

PCI DSS was the first security standard adopted by the PCI SSC, but it has not been a static standard. The PCI Security Standards Council is charged with reviewing and updating the standard to ensure that it remains effective to protect card data, by incorporating input from

stakeholders as well as technological developments in the evolution of the standard over time. Visa recognizes that no set of standards can provide an absolute guarantee of security in a changing world, and PCI DSS is not an exhaustive list of all the security practices that may be effective to safeguard card data. To our knowledge, however, no organization that has fully implemented and maintained compliance with the PCI DSS has been the victim of a data compromise event. Therefore, we believe that full compliance with the standard is a valuable component of a comprehensive security program and greatly reduces the risk of data compromise. We also believe that PCI DSS controls are highly effective in mitigating the impact of data compromise events.

Validating PCI DSS is a major milestone, but achieving and maintaining compliance requires companies to make an ongoing commitment to keeping consumers' data safe – 24 hours a day, 7 days a week, 365 days a year. While there have been a few instances where an entity that previously validated compliance was the victim of a compromise, in all compromise cases our review concluded that gaps in the compromised entity's PCI DSS controls were major contributors to the breach. As such, Visa continues to believe that standards validation is a valuable process that drives organizations to undertake the minimum steps necessary to protect cardholder data. While it is easy to focus on the failures that some entities have had with ongoing compliance, we believe it is likely that many compromises have been prevented as a result of the strenuous efforts of merchants and processors to maintain compliance with PCI DSS.

**Visa Security Initiatives**

Visa leads the payment industry in providing merchants and service providers with incentives to validate and comply with PCI DSS in order to ensure that they properly protect cardholder data. In particular, Visa launched a Compliance Acceleration Program offering $20 million in incentive payments to promote compliance among the largest U.S. merchants that account for more than two thirds of Visa annual transactions. Visa's combination of incentive payments and potential fines ultimately drove the vast majority of large U.S. merchants to validate their initial compliance with PCI DSS and to revalidate annually thereafter. At this time, approximately 90 percent of large U.S. merchants have validated PCI DSS compliance. Visa also publishes a list of service providers that have validated compliance with the PCI DSS, which has been the principal incentive in driving 80 percent of U.S. service providers to validate their compliance on an annual basis. These organizations, like Michaels, deserve credit for enhancing their security practices to meet the minimum industry standard and for validating their compliance on at least an annual basis.

Visa has also made considerable strides toward eliminating the storage by merchants and processors of authorization data, which criminals covet to perpetrate fraud. This "prohibited" data includes full magnetic stripe information, the CVV2 or "Card Verification Value 2" and PIN. Visa has executed a "drop the data" campaign over the past three years to encourage merchants to discontinue storage of prohibited data and reduce overall cardholder data storage. Additionally, Visa developed security standards for payment application vendors to support merchants in their security efforts by driving vendors to reduce data storage and provide more secure payment application products.

Visa has executed a robust data security educational campaign to engage payment system participants in the fight to protect cardholder information. This campaign includes training for financial institutions, merchants and service providers. Most large merchants, including Michaels, have attended one of Visa's security training seminars. Visa is also committed to educating system participants on emerging security threats and publishes regular security alerts

and bulletins, and holds seminars focused on data security and fraud mitigation. Visa has partnered with organizations like the National Retail Federation to promote data security among its members and commends the NRF and Michaels for their data security efforts. Visa outreach also extends to participation in industry forums on data security, media campaigns, and partnerships with other industry groups made up of merchants, such as the U.S. Chamber of Commerce. This month in Washington D.C., Visa held our third Global Security Summit, a symposium on payment security where Visa called on system participants for continued industry investment, collaboration and innovation to keep the electronic payment system secure for the future. The Global Security Summit reaffirmed the importance of ongoing compliance with security standards and highlighted opportunities to actively engage consumers in the process of fraud prevention through Visa's transaction alerts and notifications service which can not only help consumers track and manage their accounts, but also provide an early warning of potentially fraudulent activity.

**Collaboration with Law Enforcement**

Visa has maintained a long standing relationship with law enforcement agencies over the years, supporting efforts to investigate and prosecute criminals committing payment card fraud. This relationship continues and is stronger than ever today, as Visa and law enforcement agencies work together to combat cyber criminals in today's high-tech world. In 2002, Visa was a founding member of the U.S. Secret Service San Francisco Electronic Crimes Task Force and continues to actively participate in U.S. Secret Service task force groups in San Francisco, New York and Los Angeles. Visa also works closely with the Federal Bureau of Investigation's Cyber Division, United States Postal Inspection Service, State Attorneys General and the Department of Justice Computer Crime and Intellectual Property Section.

In 2004, Visa provided investigative support to federal law enforcement, which resulted in the indictment and subsequent extradition to the U.S. of Roman Vega, known online as "Boa". Roman Vega was allegedly one of the most significant high-level criminals specializing in the online sale of stolen payment card data at the time. Visa has continued with our investigative support on other high-profile investigations, including the federal prosecution of Max Ray Butler known online as the "Iceman", arrested by federal agents in 2007 and the 2008 arrest of Albert Gonzales, Maksym Yastremskiy and Aleksandr Suvorov for their scheme in which they hacked into Dave & Busters, Inc. restaurants. Visa also works closely with local law enforcement agencies and local retailers in supporting their effort to investigate and prosecute street level criminals using payment cards to commit fraud. Visa values our partnership with law enforcement and is committed to continuing to work closely with law enforcement to bring cyber criminals to justice.

**Recent Compromise Events**

After learning of data compromise events, Visa immediately begins working with the compromised entity, law enforcement, and affected client financial institutions to prevent card-related fraud. Visa notifies all potentially affected card issuing institutions and provides them with the necessary information so that they can monitor the accounts and, if necessary, advise customers to check closely all charges on their statements or cancel or reissue cards to their customers. Visa card-issuing institutions have the direct responsibility and relationship with cardholders, and because of Visa's zero liability policy for cardholders, bear most of the financial loss if fraud occurs. Visa financial institutions can best determine the appropriate action for each customer that might have been affected.

Based on Visa's findings following recent compromise events at Heartland Payment Systems and RBS WorldPay, we have taken the necessary step of removing both companies from our

online list of PCI DSS compliant service providers. In addition, we are activating our account data compromise recovery programs, which are in place to protect our system and help issuers recoup some of their losses from compromise events. Visa is committed to working with these processors so they can be reinstated to this list upon successfully revalidating their compliance and Visa is not penalizing merchants that continue to utilize these processors. Protecting our cardholders was, and remains, Visa's primary goal in responding to this incident.

**Conclusion**

In closing, securing consumer data within the U.S. economy is a shared responsibility, and every industry should deploy focused resources to protect consumer information within its care. In this regard, the payment card industry has done more than any other to provide stakeholders with the tools and guidance that they need to properly secure the data they are trusted to protect. Visa has led the industry in protecting cardholder data and stands ready to continue to support industry participants in our collective fight against the criminals that perpetrate card fraud. We look forward to working with all participants to continue to develop tools to minimize and eventually eliminate the risk of data compromise in our economy. Thank you for the opportunity to present this testimony today. I would be happy to answer any questions.