



**John Philip Coghlan
President and CEO, Visa USA
Visa Security Summit
March 8, 2007
Prepared Remarks**

Welcome to the second Visa Security Summit.

I'm honored to be joined by so many distinguished professionals from so many fields.

We are here today to talk about how we can work together to continue earning the *trust* of the customer we all share: the individual consumer.

So, I want to start our day by sharing Visa's perspectives on...

The value that trust can bring to our system,
The importance of making security a strategic priority and
The role each stakeholder—each of us--has in securing our shared system.

More than ever before, consumers are demanding that the businesses with which they transact will deliver on their expectations of iron-clad security.

In a new study released by Javelin Strategy & Research, almost eight out of 10 consumers believe identity theft is increasing. Additionally, 78 percent of consumers say they would stop shopping at a store that had experienced a data compromise.

I think that trust is emerging as one of the critical business issues of the 21st century.

The reported security breach at the TJX Companies was a stark reminder that such events can have serious and far-reaching consequences.

And every time the criminals succeed, the most valuable asset they steal isn't money -- it is trust.

My Mother called me after reading about a recent data breach. She asked me whether she should be worried about using her Visa card. Her question really crystallized the true cost of a breach. It can change the way you think about a brand and can create distrust.

In our tightly integrated system, the impact is never isolated -- it is shared by all participants in the payment system: financial institutions, payment networks, and merchants.

Yet even as we recognize the steep cost of these incidents, we must also recognize that there is much that we can do to prevent them.

Companies that adhere to the Payment Card Industry Data Security Standard significantly reduce their vulnerability to a compromise.

In fact, the majority of compromises stem from a consistent set of practices that include the storage of prohibited data and using vulnerable payment applications.

Becoming PCI compliant would remediate these obvious sources of vulnerability.

But there is more to security than just protecting downside losses. There is an upside as well.

As surely as security lapses can lead to loss -- the reverse is equally true. There is enormous opportunity for businesses to use trust as a way to differentiate themselves and, consequently, to build client loyalty and grow more rapidly.

According to a study by the CMO Council, virtually no industry or brand has succeeded in establishing a reputation for being trustworthy when it comes to security.

That gap between what customers *perceive* companies are doing and what they want companies to be doing -- represents a huge opportunity.

Where opportunity like this exists, investment should follow -- and in this day and age an investment in trust is just good business.

The path starts with all stakeholders making security a top priority.

There is too much at stake to allow security to be an afterthought. It must become an ingrained part of business culture.

Security must move out of the back office and into the board room.

Corporate officers must apply the same rigor to security as they do to their financial controls -- from small proprietorships to giant multinational businesses.

That does not mean that every CEO needs to become an IT specialist.

But it does mean that no CEO can afford to abdicate responsibility for security to their IT or risk management departments.

This kind of engagement does require a commitment of resources to invest in technology and rethink business process for data storage.

But in the end, resources spent on security are not simply an additional cost. They are a necessary investment that can generate real returns.

The Javelin poll released today shows that 85 percent of consumers are likely to increase their shopping with a merchant that is a known for its security leadership.

But it's not just merchants who have to step up to this challenge. We *all* have a role to play.

Financial institutions must use the tools available to them to keep fraud low and protect cardholders.

In addition to their own risk management tools, many take advantage of sophisticated capabilities like Visa's Advanced Authorization.

It's patented technology that uses the phenomenal array of data that we have to evaluate and risk-score a transaction in-flight, in real time -- helping financial institutions stop a fraudulent transaction before it can occur!

Government can help by exploring a national, risk-based approach to regulation in this area.

We will work closely with Congressional leaders over the coming months to protect consumers without unnecessarily hobbling the system that serves them.

Hardware and software vendors play a vital role by stopping the development or sale of technology that inappropriately stores or inadequately protects sensitive data.

Some devices in use today store card data -- sometimes without the merchant even knowing it.

That is why in 2005 Visa introduced our Payment Application Best Practices program, which provides guidelines for developers to follow when creating new payment software.

And, of course, for merchants and processors, they must protect cardholder data and use technology to screen for fraud.

I'm talking about technologies like Verified by Visa that reduce operational expenses by protecting merchants from fraud-related chargebacks.

All stakeholders must play their part. After all, it is their very existence as a business that is at risk.

But let me turn to the role of Visa -- and the other payment networks -- who must play a lead role in making payments secure.

With so much at stake, we know we must protect the system we have helped to build.

So for three decades, we have implemented anti-fraud programs, set security standards and provided the means for system participants to protect themselves.

Our current "layers" of security have helped bring our *net* fraud-to-volume ratio down to just 6 cents for every \$100 spent -- near its historic low.

But as overall sales volume increases, GROSS fraud levels are rising.

And that is the metric on which we must focus --responding with new ways to drive fraud out of the system.

There are two principal ways we can drive fraud lower:

1. Technology we can apply to the physical system, and
2. Policies we can use to guide system-wide behavior.

On the technology front, Visa is investing heavily to prevent criminals from accessing card or account information -- and rendering that data useless if stolen.

Current fraud tools rely on static information such as card verification codes, PINs and passwords -- and these tools have been very effective.

But criminals aren't static.

In the future, our system will have to rely on more adaptive forms of security.

We believe one promising approach is to introduce *dynamic information* into the transaction.

By making individual elements of a transaction dynamic, we can protect the underlying account data.

For example, if we apply a unique value to a card or another unique value to each transaction -- and then use the network to authenticate that information in real-time --the security of that transaction goes up significantly.

This approach makes it much harder for criminals to use stolen data to commit fraud.

Even if thieves create a counterfeit card with stolen data, fraud is stopped because the transaction won't occur without the dynamic information being supplied and authenticated.

It's an example of how our cards and our network can work together to drive down fraud, efficiently and effectively.

Technology like this is already in use on all Visa Contactless cards, through authentication of a Dynamic Card Verification Value -- or "D-C-V-V".

We will be working with issuing financial institutions and merchants to pilot other forms of dynamic authorization in the coming months.

But as we converge on solutions, they must be *industry-wide* solutions; Visa cannot do it alone. New solutions will require adoption by merchants and processors, and issuance by financial institutions.

There must be a shared commitment to prevention at all points in the transaction -- from swipe to settlement.

In addition to technology, we must apply the right policies to address improper storage of system data.

Last year, we partnered with the U.S. Chamber of Commerce on an educational effort to help merchants protect themselves and their customers.

This year, we're also partnering with the National Federation of Independent Businesses on security education.

And, since 2001, Visa has required any entity that touches data to be compliant with industry security standards.

We have made some progress -- but inadequate progress -- working with merchants and processors to boost data security.

In the last year, PCI compliance among the largest merchants doubled, from less than 15 percent to more than one-third. Substantially more are in the validation process right now.

These are merchants who together process about 50% of Visa transactions.

Of the companies whose business it is to process Visa transactions, more than 85 percent have been validated as PCI-compliant. We applaud those entities that are already making the necessary investments in security.

But that still leaves us --today -- with less than *half* of the top merchants as certified compliant.

That is simply *not good enough* -- and that is why we are moving forward with new approaches to convince merchants to accelerate their efforts to comply with these important standards.

Last December, Visa announced its PCI Compliance Acceleration program -- and became the first in the industry to adopt a program with fines for non-compliance *as well as incentives* for those reaching compliance. Visa is planning to pay out more than \$20 million in incentives this year.

As part of the acceleration program, Visa is also adopting a new policy related to interchange fees. Visa's best interchange rates *will only* be available to merchants -- through their acquiring financial institutions -- *if* they validate PCI compliance by September 30, 2007.

For the largest merchants, the cost could be tens of millions of dollars.

It is our hope that these programs will provide powerful market-based incentives for all entities to get compliant... and stay compliant.

Full compliance with these security standards is absolutely critical to maintaining the trust that all the participants have placed in the Visa system.

But as we work to increase compliance -- we also have to prepare for additional compromises.

An important part of successfully managing any breach is the rapid disclosure of the event by the compromised entity.

This simple act, done early, is essential to protect consumers from misuse of their information, protect businesses from financial loss, and protect the entire system from the erosion of trust.

As we go forward, Visa will actively encourage compromised entities to accelerate the timing of their disclosure. We believe they have a responsibility to do so -- to their customers and to the system as a whole.

And we will continue to provide our own financial institution clients and our regulators with all of the information we can appropriately share -- as quickly as we can share it -- so they can protect their cardholders, monitor for fraud and limit financial loss.

We believe that more information, provided faster, will help build and maintain the confidence of all parties in the system.

Finally, we must be smart about how we target criminal activity. That means taking a

risk-based approach to fighting fraud.

Fraud is not random; it's concentrated in specific segments. And losses are concentrated in an extremely small percentage of transactions. We should focus our efforts on areas where it's concentrated.

Today, more than 80 percent of the dollars lost to fraud come from just 20 percent of fraudulent transactions.

By singling out the highest-risk transactions, we can apply targeted security solutions in those areas -- and knock out a disproportionate amount of fraud.

This approach helps us to get the most out of each dollar we invest in security -- and, very importantly -- it will achieve results faster.

The other day, I was shopping online for a cell phone for my daughter's birthday.

As I considered buying it from a merchant I didn't recognize, it struck me how remarkable the entire system truly is -- hundreds of millions of consumers in all parts of the world, sending money over a vast network to transact with millions of businesses worldwide.

I thought about what makes it all possible -- the technology, innovation and the ingenuity it takes to make the infrastructure work.

But what really powers the machine is trust.

I send money to a merchant I never see, over a network I cannot touch -- and I trust that the transaction will happen as I expect it, and that I will be protected.

If I have that trust, I will make those transactions over and over again. Commerce will flourish, and growth and efficiency are both spurred. Our job is to make sure that trust is protected. And achieving that goal requires unity of purpose. We must work together.

So over the course of today, as you hear experts discuss different perspectives on how we can advance payment security, I'd like you to ask yourself:

Are you willing to make the necessary investment to safeguard that trust?

Are you willing to work collaboratively to do so?

And, importantly, are you willing to bear the price of failure?

At Visa, we are committed to succeed. We are willing to make that investment, and to work alongside you to protect this wonderful payment system and the hundreds of millions of consumers who place their trust in it.

I know that you will join us.

Thank you for investing your time, energy, and ideas with me in this vital endeavor.