

Securing the Payments System

The facts about fraud prevention



Contents

Introduction	3
Visa's Security Program	4
Fraud Types and Threats	6
Fraud Statistics and Research	7
Visa's Security Agenda for Australia	8
The Payment Card Data Security Standard	9
Chip Cards	10
Zero Liability	11
Verified by Visa	12
CVV2	13
Cardholder Safety Tips	14
Online Shopping Tips	15

For more information

Visa Corporate Relations, Australia, New Zealand & South Pacific
Telephone: +61 (0)2 9253 8817

Email: ausinfo@visa.com

Website: www.visa.com.au

November 2009

Introduction



Protecting cardholders from fraud has always been one of Visa's highest priorities. That's why we have invested millions of dollars in state-of-the-art anti-fraud technologies, and we continue to develop and deploy new programs to enhance security.

Visa's efforts have kept global fraud rates steady near historic lows, enabling cardholders to use Visa with confidence. In fact, with technological innovations and advances in risk management, fraud rates have declined by more than two-thirds in the past two decades.

In Australia, Visa is working with the industry to implement a comprehensive seven-point security agenda to strengthen the payments system.

As part of this, Visa will be migrating to 100 percent chip and PIN technology across all domestically-issued Visa credit, debit and prepaid cards by 2013. All merchant sales terminals will also be chip capable and activated, and cardholders will be required to use PINs (Personal Identification Numbers) instead of signatures to authorise a transaction.

Apart from being effective in preventing counterfeit fraud, chip offers banks and merchants the ability to provide their customers with benefits such as faster transactions, innovations such as contactless payments and the opportunity to store information such as reward programs on their cards.

Visa is also developing a coordinated approach to online and other Card-Not-Present fraud and driving merchant compliance with global data security standards. These measures should reduce fraud levels and ensure Australia's payment system remains among the safest in the world.

Chris Clark

General Manager, Australia, New Zealand and South Pacific
Visa

Visa's Security Program

Today's data thieves are highly sophisticated in their technological expertise and their understanding of the payment infrastructure. They are smart, nimble and determined - moving quickly to take advantage of any new opportunity to perpetrate fraud globally.

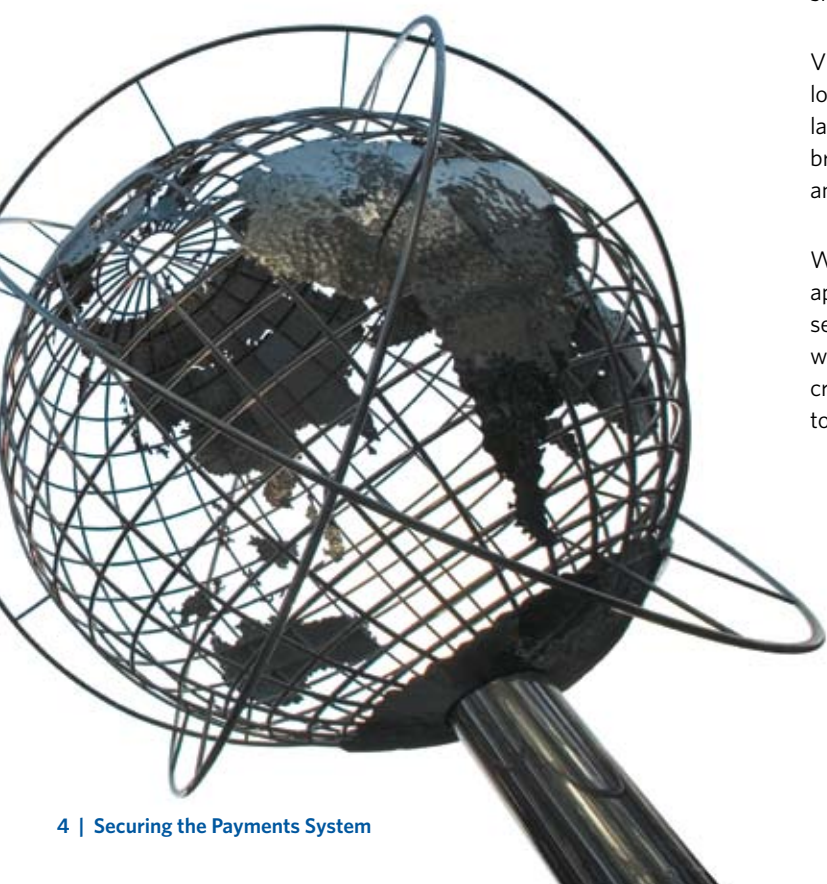
The impact these criminals can have on commerce is real. Although payment card fraud rates have remained stable, any incident of fraud can erode the trust of cardholders and merchants. Put simply, today's criminals - data thieves, hackers and phishers - are dangerous because they don't just steal money, they steal peace of mind.

To counter this threat, every entity with a stake in the electronic payments network must be fully committed to protecting the system 24 hours a day.

Visa's approach is based on the belief that the only effective way to fight fraud is to employ multiple layers of security. Simply put, there is no "silver bullet" that will erase fraud. Criminals attack the payment system from many directions using multiple tools and tactics. Visa works to protect each link within its control and works with others in the payment chain with an aim to ensure there is no single point of failure - no weak link.

Visa seeks to address all forms of fraud, including counterfeiting, lost and stolen, card-not-present, and identity theft. That is what layers is all about - making sure that even if criminals succeed in breaching one layer, they find another locked door in front of them, another, and another and another.

We have aligned our myriad security efforts into a comprehensive approach that is designed to remove the weaknesses fraudsters seek to exploit. Each policy, program and technology application within Visa's security layers work in concert to achieve a single, critical goal: creating and maintaining the safest, most secure way to pay.



Visa's solutions

Visa has developed a range of tools and services to allow fraud to be managed effectively. These include:

VISA CARD SECURITY FEATURES

The Visa card itself has a number of built-in security features designed to help card issuers and merchants recognize a real card from a counterfeit one. These include the magnetic stripe, embossing, dove hologram and three-digit Cardholder Verification Value (CVV2). When a merchant collects the CVV2 in an offline transaction such as during an internet, mail order or telephone transaction, the card issuer can verify that the data is genuine.

CHIP TECHNOLOGY

Visa is working to bring chip technology to cardholders and merchant point of sale terminals. A chip card is a card that contains an embedded microcomputer chip that stores and processes data. The chip cannot be counterfeited, because some of the data necessary for counterfeiting cannot be copied from the genuine chip.

VERIFIED BY VISA PROGRAM

Verified by Visa is a global authentication program providing an added level of security for online transactions. The Verified by Visa service verifies cardholder identity in real-time through the use of a password so customers can shop more confidently and merchants can accept Visa cards with peace of mind.

ZERO LIABILITY

Visa's Zero Liability policy is our guarantee that cardholders will not be held responsible for fraudulent charges made with their Visa payment card. Visa's cardholder protection policy requires all financial institutions issuing Visa products to extend provisional credit for losses from unauthorized card use within five business days of notification of the loss.

VISA'S ACCOUNT INFORMATION SECURITY PROGRAM (AIS)

AIS is a global program requiring merchants to make their virtual and physical environments more secure, thereby helping protect against hacks. This program provides merchants with an easy-to-use toolkit aimed to help them understand and implement processes that protect cardholder account and transaction data. The program includes global standards, a best practices guide, and a self-assessment questionnaire providing key information and requirements.

Visa has aligned its AIS program requirements with other payment providers to provide the global Payment Card Industry Data Security Standards (PCI DSS). Merchants and service providers are able to assess the status of their security by using a single set of security standards.

ANTI-PHISHING INITIATIVES

Visa plays an active role against scams such as "phishing" and "spoofing", where emails and fake websites are used to trick consumers into submitting personal, financial or password data. Visa works closely with industry partners and law enforcement agencies to shut down phishing websites. In the past year alone, Visa deactivated 85 percent of reported phishing attacks within 48 hours of notification.¹ Visa believes that the key to stopping this type of fraud is through education. Consumers are urged to report any emails and fake websites claiming to be from Visa or their issuing financial institution that request their personal account information to phishing@visa.com.

INDUSTRY COOPERATION

Global standards are a vital part of a secure and efficient payments industry. Visa donates many of its security initiatives to the industry and participates in a number of industry work groups aimed at enhancing industry wide security.

¹ Source: RSA Repository 15 October 2007 - 15 October 2008 Data

Fraud Types and Threats

There are three major types of payment card fraud – counterfeit, card-not-present and lost and stolen card fraud. In addition, hacking and phishing are two of the common methods criminals use to obtain cardholder information to commit fraud.

COUNTERFEIT FRAUD

Counterfeiting involves making replicas of legitimate credit, debit and prepaid cards by copying or “skimming” the data contained in a card’s magnetic stripe. Using this “skimmed” information, criminals manufacture fake or counterfeit cards and use them for fraudulent purposes.

CARD-NOT-PRESENT FRAUD (CNP)

This type of fraud is committed without the actual use of a card - for instance in online, phone or mail-order transactions. CNP fraud on Australian issued cards has increased in recent times². Fraudsters like this type of fraud because they do not have to be physically present to commit the crime.

LOST AND STOLEN FRAUD

This type of fraud is incurred on cards that have been reported either lost or stolen previously by the genuine cardholder.

HACKING

Criminals are becoming increasingly tech-savvy and have found ways to break into a company’s computer system to gain access to confidential customer information. This information can then be used to commit card-not-present fraud or to make counterfeit cards.

PHISHING

Fraudsters looking to gather financial information have developed a way to lure unsuspecting victims: they go “phishing.” Phishing is the creation of email messages and web pages that are replicas of existing legitimate sites and businesses. These emails are used to trick users into submitting personal, financial or password data. These emails often ask for information such as credit card numbers, bank account information and passwords that will be used to commit fraud.

² Payment Fraud Data, Australian Payments Clearing Association, 12 months ended 30 June 2008.

Fraud Statistics and Research

GLOBAL CARD FRAUD

Global card fraud has been on a downward trend since the 1990s as a percentage of total card transactions, according to The Nilson Report³.

Fraud worldwide on all credit, debit and prepaid cards equalled 4.7 cents per \$100 in total volume of purchases and cash in 2007, down from 6.1 cents in 1993. Card Not Present (CNP) fraud (fraud committed online, over the telephone or via mail order when the card is not physically present at point of sale) accounted for the largest source of monetary losses, Nilson said.



³ The Nilson Report, Issue 915, November 2008

AUSTRALIAN FRAUD DATA

Data on Australian payments fraud collected by the Australian Payments Clearing Association (APCA) shows that fraud remains a fraction of an overall increasing number of payments.

In the 12 months to December 2008, fraud across credit and charge cards accounted for 5.3 cents of every \$100 transacted⁴. Credit and charge card fraud in Australia amounted to A\$144.7 million in the 12 months to December 2008 out of a total of A\$272.0 billion worth of transactions conducted. Card Not Present fraud was the most common type of payment card fraud during the period, followed by counterfeit card fraud.

APCA said Australia's total rate of fraud remains low when compared to other countries. With an incidence of one in every 10,000, the chance of becoming a victim of payments card fraud is relatively low. For more information, visit www.apca.com.au.

⁴ Payment Fraud Data, Australian Payments Clearing Association, 12 months ended 31 December 2008. The data relates to financial institutions which include banks, building societies and credit unions.

Visa's Security Agenda for Australia

A SEVEN-POINT PLAN

Visa is working with Australian financial institutions and merchant communities to implement a comprehensive five-year agenda to strengthen the security of the payments system in Australia.

The agenda consists of seven key security initiatives which will be implemented to fight fraud and keep fraud rates low into the future. These are:

- Moving to 100 percent chip card issuance. By 1 January 2010, banks and other financial institutions must issue all new Visa credit cards on chip; by 1 January 2011 all new Visa debit and reloadable prepaid cards must be on chip; and by 1 April 2013, 100 percent of all Visa cards must be on chip. In addition, from 1 January 2012 the chips used in new Visa cards must support Dynamic Data Authentication (DDA).
- Ensuring all merchant acceptance terminals must be chip capable and activated by 1 April 2012.
- Ensuring all new Automated Teller Machines (ATMs) commissioned must be chip capable by 1 January 2011.
- Introducing a broad rollout of PIN (Personal Identification Number) verification for all domestic transactions, with signatures no longer accepted from 1 April 2013.

- Issuers must enrol all Visa cards for Verified by Visa, a free service for cardholders that provides a password for secure online shopping, by 1 April 2012.
- All merchants who take online, telephone and mail order transactions must check the three-digit card verification code (known as CVV2) from 1 January 2011.
- Small and medium sized (Level 4) merchants will be required to implement higher levels of data security. Acquiring banks will be required to provide Visa with a program for their merchants to comply with the Payment Card Industry Data Security Standard (PCI DSS) by 30 April 2010 that includes a strategy for risk profiling, merchant education and compliance reporting twice per year.

These initiatives are aimed at addressing online fraud; fraud resulting from lost, stolen and counterfeit cards and from the possible theft of personal financial information.

All of the initiatives will provide greater protection against fraud for cardholders, merchants and financial institutions, while some will also help to reduce the time it takes to make an electronic transaction.



The Payment Card Industry Data Security Standard (PCI DSS)

PROTECTING CARDHOLDER ACCOUNT DATA

When cardholders present their Visa card at the point of sale, over the internet, on the phone, or through the mail, they want assurance that their account information is safe.

That's why all merchants and service providers who store, process or transmit Visa cardholder data must adhere to the Payment Card Industry Data Security Standard (PCI DSS), which offers a single approach to safeguarding sensitive data for all card brands.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

The program consists of 12 key requirements:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security.

To check whether they meet the PCI DSS standards, organizations can complete an online Self-Assessment Questionnaire. Visa can enforce compliance using financial penalties on all acquirers.

To help organizations comply with the PCI DSS standards, Visa has developed the Account Information Security (AIS) program. To learn more about the program, merchants should contact their acquiring bank or visit <http://www.visa-asia.com/ap/au/merchants/riskmgmt/ais.shtml>.

Chip Cards



WHAT IS A CHIP CARD OR A SMART CARD?

Chip cards are payment cards carrying an embedded microchip. The computing power of the chip means that smart cards can offer new payment options and services, additional levels of security, and more convenience and choice.

HOW DO THEY MAKE PAYMENTS MORE SECURE?

Chip cards, when used in conjunction with a personal identification number (PIN), are a solution to counterfeit and lost and stolen card fraud. The chip prevents the card from being counterfeited and the PIN uniquely identifies the owner of the card and prevents it from being used by someone else if lost or stolen. When a chip card is used at the point of sale, the transaction message sent by the chip card to authorize the transaction does not contain any data that can be used to counterfeit a chip or conduct an unauthorized chip transaction reusing the data from a previous transaction.

WHAT IS EMV?

EMV stands for Europay, MasterCard, Visa, the three organizations that developed and established EMV as the global standard for chip-based credit and debit transactions. The EMV standard helps to maximize security and global interoperability so that Visa cards can continue to be accepted around the world.

WHAT OTHER BENEFITS DO CHIP CARDS OFFER?

In addition to protecting against fraud, chip cards help to consolidate your wallet through the ability to combine multiple functions on one card, such as reward programs, discounts and special offers.

OVERSEAS EXPERIENCE

Chip card technology is already being used widely in Europe and Asia and has proven to be extremely effective in reducing fraud. The UK's Centre for Retail Research conducted a major survey of retailers and found that 81 percent experienced a reduction in fraud and 62 percent found that transaction times were quicker⁵.

As many countries migrate to chip and PIN technology, cardholders travelling overseas should be aware that if their card has been configured as a PIN preferring card by their issuer, they may need to use that PIN to verify their chip card transactions.

⁵ Chip and PIN in Europe, survey commissioned by Visa Europe, 2008

Zero Liability

Cardholders can use their Visa card to shop with confidence because Visa's Zero Liability policy is our guarantee that cardholders will not be held responsible for fraudulent charges made with a Visa payment card.

Cardholders should take the time to review their monthly statement and immediately report any suspicious charges to their financial institution. If applicable, the financial institution may remove fraudulent transactions or extend provisional credit for losses from unauthorized card use.

Visa's cardholder protection policy requires all financial institutions issuing Visa products to extend provisional credit for losses from unauthorized card use within five business days of notification of the loss. Cardholders should contact their issuing bank for more information.



Verified by Visa



Verified by Visa is an easy to use password protected service that verifies a cardholder's identity when they shop online. Quite simply, it requires the cardholder to provide a personal password when paying for goods online with their Visa card just as they would provide a PIN or signature at point of sale.

Verified by Visa provides proof that a genuine cardholder and a genuine Visa retailer are taking part in the transaction, protecting them against the risk of their card being used fraudulently on the internet. For the retailer it provides a guarantee that the cardholder is who they say they are and reduces the likelihood of fraudulent transactions.

The goal of Verified by Visa is to increase the level of consumer trust and confidence in online shopping as well as to reduce disputes and fraudulent activity.

HOW DOES VERIFIED BY VISA WORK?

The cardholder can sign up for Verified by Visa either by signing up when shopping online when prompted by their issuing bank during the online buying procedure or with their bank through a simple one-off registration procedure. They will be asked by their bank to answer a series of security questions, to select a password to authenticate themselves and a secret phrase which will be displayed during the verification process to let the cardholder know they are dealing with a legitimate retailer.

- Once signed up the cardholder can shop with confidence at any participating online store
- When shopping online, the cardholder selects the goods and services they wish to purchase and goes to the checkout page
- They enter their Visa card number and a pop up screen from their bank appears asking for their password
- Their bank verifies the password is authentic and the transaction is completed giving the retailer and the cardholder the confidence that the identity of each party has been authenticated.

Online retailers who participate in the Verified by Visa program can receive protection from fraud related chargebacks.

Verified by Visa is built upon the technology platform called Three-Domain (3-D) Secure. The 3-D Secure technical specifications and protocol uses Secure Sockets Layer (SSL) encryption that is already supported by the majority of online merchants.

For more information about Verified by Visa visit <http://www.visa-asia.com/ap/au/cardholders/security/vbv.shtml>

Card Verification Value 2 (CVV2)

CVV2, which stands for Card Verification Value 2, is an important security feature for merchants who accept Visa cards as payment over the telephone or online. Located on the back of all Visa cards, the CVV2 code consists of the last three digits either printed on the signature panel or on a white box to the right of the signature panel.

In the card-not-present sales environment, CVV2 is an excellent tool for verifying that the customer has a legitimate Visa card in hand at the time of the sales order.

HOW IS CVV2 BENEFICIAL IN AN E-COMMERCE ENVIRONMENT?

Visa and the issuing banks provide a real-time check of the CVV2 code. This helps e-Commerce merchants verify that the person making the purchase actually has a genuine card in their possession.

If a purchaser only has the 16-digit credit card number and the expiry date, they may not have the card, highlighting a potentially fraudulent transaction. CVV2 is not a full identification of the cardholder but it does present a significant barrier to the most common types of e-Commerce fraud. The CVV2 can also help prevent fraud attacks using large-scale generation of card numbers.

MERCHANTS WHO USE CVV2 BENEFIT IN A NUMBER OF WAYS:

- Enhanced fraud protection - CVV2 can help a merchant differentiate between good customers and fraudsters who operate anonymously. It allows them to make a more informed decision before completing a non-face-to-face transaction.
- Reduced chargebacks - using CVV2 potentially reduces fraud-related chargeback volume. Reduced fraud-related chargebacks translate into maximized profitability.
- Improved bottom line - for card-not-present merchants, fraudulent transactions can lead to lost revenue and can also mean extra processing time and costs, which often narrow profit margins. CVV2 complements current fraud detection tools to provide a greater opportunity to control losses and operating costs.



Cardholder Safety Tips

Here are some basic fraud prevention steps to help cardholders stay secure when using Visa payment cards:

ON RECEIVING YOUR CARD:

- Sign your card on the signature panel as soon as you receive it.
- Never write down your personal identification number (PIN) - memorize it.
- If at all possible, do not let your card out of your sight.
- Make a record of your credit card account numbers and telephone numbers for reporting lost or stolen cards. Keep that list in a safe place.
- When selecting a PIN, always avoid the obvious - your name, telephone number, or date of birth, or any combination of these.
- Never disclose your PIN to anyone. No one from a financial institution, the police, or a merchant should ask for your PIN. You are the only person who should know it.

SAFE CARD USE:

- Keep copies of your ATM receipts.
- When your card has become stuck inside an ATM machine, be suspicious of anyone offering their help, even if they appear to be a bank security officer. Criminals can obtain your PIN by several means (shoulder surfing or straightforward questioning), then retrieve your jammed card from the ATM and use it to withdraw funds.
- When traveling it is advisable that you only take one ATM card and memorize the PIN.
- Protect your cards as if they were cash. Do not leave them unattended anywhere, such as in a car, bar, nightclub or on the beach.

- Always check sales vouchers including the purchase amount when you sign them.
- Keep copies of sales vouchers and ATM receipts.
- Never give your credit card number over the phone, unless you are dealing with a reputable company, or you have initiated the call yourself.
- Always check your billing statement, especially after a trip. Check all transactions, even the small ones, because criminals try "testing out" stolen accounts by buying inexpensive items rather than large ones.
- Be careful when giving out your credit card number over the telephone. Ask for information in writing from the company making the offer.
- If you feel pressured by a telemarketing salesperson, be suspicious. Never give out your account number unless you've decided to make a purchase.
- Do not volunteer any personal information when you use your credit card, other than your ID document, which may be requested.
- Know who has access to your cards. If your credit card is borrowed by a family member (spouse, child, parent), with or without your knowledge, you may be responsible for their purchase/cash withdrawal.

IF SOMETHING GOES WRONG:

Report lost or stolen cards immediately. You can call [Visa Global Customer Assistance](#) from anywhere in the world via the toll-free numbers listed on the Visa website, or your card issuer.

Online Shopping Tips

Here are some basic tips for shopping safely online with your Visa payment card:

VISA'S ZERO LIABILITY

Visa's Zero Liability policy is a guarantee that you will not be held responsible for fraudulent charges made with your Visa payment card.

REGISTER FOR VERIFIED BY VISA

Verified by Visa is a service that allows you to use a personal password to protect your Visa card when you shop online, giving you added reassurance.

USE A SECURE WEB BROWSER

Use a secure browser - look for an "s" after the "http" in the web page address or URL.

KEEP YOUR PASSWORD SECRET

Some online stores require you to register a user name and password before buying an item. Just as you keep your ATM code secret, keep your password secret from outside parties. When shopping with Verified by Visa, keep your Verified by Visa password secret.

USE THE INTERNET TO COMPARE BETWEEN SHOPS BEFORE BUYING ONLINE

Compare products and prices before you buy to find your item at the best price.

PROTECT YOUR CARD DETAILS

Only give your Visa card details when making purchases - do not provide them for any other reason.

CHECK DELIVERY AND RETURN POLICIES

Before completing an online transaction, read the delivery and return policies on the online store's home page. Find out if you can return items and who bears the cost.

NEVER SEND PAYMENT INFORMATION VIA EMAIL

Information that travels over the internet (such as email) is not fully protected from being read by outside parties. Most reputable merchant sites use encryption technologies that will protect your private data from being accessed by others as you conduct an online transaction.

KEEP A RECORD OF YOUR TRANSACTIONS

Just as you save store receipts, you should keep records of your online purchases. Back up your transaction by saving and/or printing the order confirmation.

REVIEW YOUR MONTHLY ACCOUNT STATEMENT THOROUGHLY

Monitor your monthly statements, especially after an overseas trip. Check all transactions, even the small ones, because criminals try "testing out" stolen accounts by buying inexpensive items rather than large ones. Immediately investigate suspicious activity to prevent any possible additional fraud before it occurs. Promptly notify your financial institution of any suspicious email activities.

