VISA

Securing Payments

Building Robust Global Commerce

Contents

Executive Summary

Visa Solutions: Securing the Future of Electronic Payments

Trust is an essential component of financial systems. Establishing and maintaining trust is an endless battle that pits financial institutions and governments against would-be criminals.

This paper describes an important part of this battle —how transactions are moving away from physical cash and cheques to electronic systems and how Visa stays on the leading edge of preventing criminals from exploiting electronic payments.

The evolution of electronic payments recently reached a milestone. A study released by the Federal Reserve System of the United States in December 2004 revealed that electronic transactions in the US—including debit cards, credit cards and other electronic payment forms—had exceeded cheque payments for the first time in history. While the US is only one of the many markets that Visa serves, it is a clear indicator of a global movement toward electronic payment. Visa sees similar trends in other markets and it is generally accepted that this trend will continue.

This rapidly changing landscape presents new challenges for those responsible for maintaining a safe, sound and predictable international payments network. Visa takes those challenges seriously and makes security its highest priority. The world trusts Visa to provide the most secure and reliable means to pay and be paid, stimulating growth and generating opportunities. Visa's goal is to connect buyers, sellers and member banks in the most secure environment it can possibly create. This paper explains the extensive measures Visa takes to make electronic payments secure, not only through its own payment network, but also for similar networks around the world.

The benefits of a healthy, safe and efficient electronic payment system are increasingly known: greater economic growth, new jobs, more tourism, movement of additional people into the banking system, and a continued expansion of e-commerce that brings buyers and sellers together across geographic boundaries.

Given the enormous challenges involved, Visa's security efforts are aimed at achieving basic but essential goals. Visa goes to extraordinary lengths to make sure potentially sensitive material—the card itself, the card number and the personal identification number or PIN—remain in the control of only one person, the actual cardholder. It is Visa's goal that when a transaction occurs on a Visa account, the cardholder, the merchant and the relevant banks can be sure that the valid cardholder has actually initiated and approved the transaction. As this paper explains, Visa has devised a number of ways to authenticate credit and debit card purchases, protecting both buyer and seller, especially for the growing number of sales where the buyer and seller do not meet face to face.

Visa's commitment to security rests on three pillars that support everything it does on behalf of its cardholders, participating merchants and member financial institutions:

Reliability

Visa sets as a baseline a network reliability standard of 99.999%. This standard enables the system to work efficiently, effectively and securely, and is a key element in protecting all stakeholders against financial loss.

Collaboration

Visa employs industry experts who collaborate closely with its members to combat fraudulent activity, which is often perpetrated by organised criminals. In addition, Visa works with national and international law enforcement bodies, merchants and leading edge technology providers in order to minimise risk whilst allowing cardholders to freely use their cards wherever they may be.

Leadership

Visa donates many of its solutions to the industry to increase security of all payment systems. Ultimately, this helps strengthen the foundations of global commerce.

The success of these efforts can be measured in a number of ways. Statistically, as of the four quarters ended September 30th 2004, fraud accounts for less than seven cents for every US$100 in transactions, half the rate of 1993. Most importantly, success is measured by the growing confidence people show in paying electronically and the rapid rate at which electronic payments are being adopted. This paper explains what Visa is doing to secure that payment system and help build a stronger, more robust global economy.

Trust. It is the core principle behind financial services.

Visa and Trust

Think of the evolution of money from shells and precious metals to coins, paper money, cheques, and electronic systems. For commerce to take place, buyers and sellers must trust the value of the exchange. They must trust the ways they can transport, store and account for their funds. A central role of government—in conjunction with financial institutions in more modern times—has always been to establish and maintain trust in the means of exchange, and to account for the wealth of an economy in a trustworthy way.

The concepts of trust are ingrained in our society: the government imprimatur that creates a banknote out of mere paper, the stagecoach lockbox, the bank vault, the padlock symbol at the bottom of a web browser.

Yet we have as many contrasting images: the counterfeiter falsifying bills, the bandit, the bank robber, and the computer hacker.

There is an endless battle of innovation, with government and the financial services industry creating new ways to ensure the trustworthiness of exchange, and criminals finding new ways to crack the code.

This paper describes an important part of this battle—how transactions are moving away from physical cash and cheques to electronic systems, where risks exist, and how Visa stays on the leading edge of preventing criminals from exploiting electronic payments.

Every time someone says, “Put it on my Visa card,” they are expressing their trust in the world’s largest electronic payments network to link the cardholder, the merchant and their respective banks successfully, and to do it quickly, securely and reliably.

Whether they are individuals or institutions, more buyers and sellers are turning to electronic payments than ever before, choosing the convenience, efficiency and security of an electronic transaction over payment by cash or cheque. Throughout its history, Visa has earned the trust of buyers and sellers by bringing innovation and advanced technology to the development of electronic payment products.

At the heart of everything Visa does is one fundamental belief: protecting cardholders. People trust the Visa brand because it makes buying and selling safe and secure. By adhering to that core value, Visa not only protects the cardholder, but also contributes to the business success of the merchants and financial institutions that must be linked instantly and seamlessly millions of times each day. Visa takes a comprehensive approach to security—ensuring that fraud is prevented whenever possible and detected and dealt with when it does occur. To that end, Visa has made an unwavering commitment to the security of data and created a body of industry standards that has infused the marketplace—real and virtual—with a sense of trust.

A healthy global economy demands a secure payment system. Visa’s financial tools and expertise help fuel economic growth and create social benefits around the world. From a satisfied shopper to a successful merchant to a more robust banking system, electronic transactions are at the heart of a vibrant economy. Indeed, the security of electronic payments has been one of the driving forces behind the expansion of international commerce, bringing buyers and sellers together across geographies via the internet. As Visa is committed to protecting the cardholder and merchant in all environments, it is the most secure way to pay and be paid in the world. Through Visa's leadership in risk management and work with law enforcement, technology, security and payment-related agencies, fraud levels today stand at less than seven cents for every US$100 in Visa card volume, well below the level of the early 1990s.

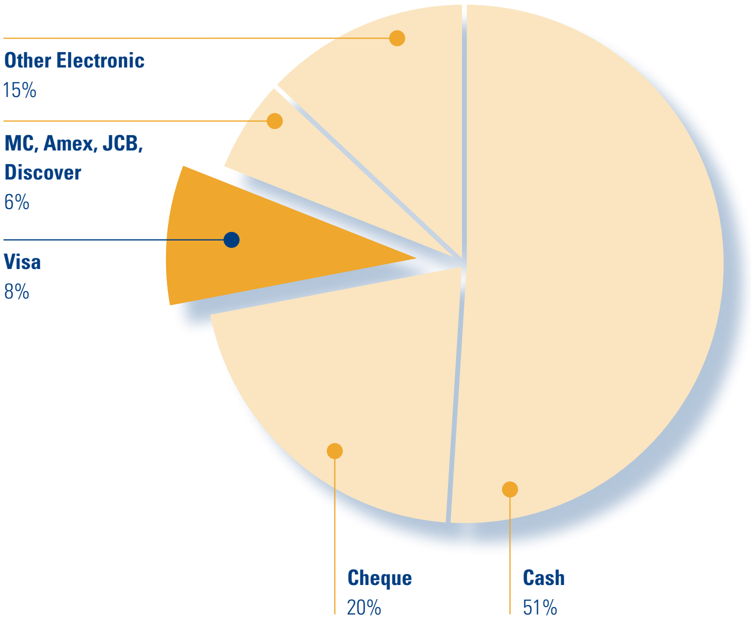
Building trust in a payment system calls for constant vigilance, innovation and commitment. Visa can never afford to lower its guard in staying ahead of criminals who have their own commitment to compromising and exploiting the system for their own gain. And Visa never will.

With 21,000 member financial institutions and their affiliated merchants, Visa is the most widely used form of electronic payment in the world. It is Visa's vision to be "the way the world pays". Visa products and services allow buyers and sellers to conduct commerce with choice, ease and confidence in both the physical and virtual worlds—anywhere, anytime and any way.

Figure 1

Share of Personal Consumption Expenditure (PCE), 2004

Source: Global Insight



But that cannot happen unless buyers, sellers and banks trust the system, and that does not happen unless they believe the system is secure.

Defining the Issue

The millions of transactions that take place every day between customers and the providers of goods and services make up the world of retail payment systems. The standard measurement of this activity is known as Personal Consumption Expenditure (PCE).[1] As shown in Figure 1, electronic payment systems accounted for approximately 29% of global PCE in 2004, compared with roughly 51% for cash and 20% for cheques. Roughly half of the electronic payments, or 14% of total PCE, were made with some form of payment card (eg, Visa, MasterCard, American Express, Discover, JCB).

There are risks involved in all types of payment systems. Retail payment systems, in particular, face three types of risk, often referred to as systemic risk:

Technology Risk: Network Failure
Earthquakes. Hurricanes. Terrorist attacks. Viruses. Power blackouts. Electronic payment systems must be built to maintain their integrity and operability in the face of these and other threats. They must also have contingency plans to maintain the security of financial records and other critical data in the event of a system failure. Their reliability must be as close to 100% as possible in order to maintain the degree of trust that is critical to stakeholder confidence. To this end, business planning rules, network connections, hardware, software applications, data storage and backup systems must be constantly reviewed and tested against all contingencies.

[1] Personal Consumption Expenditure (PCE) represents the market value of all goods and services purchased by households and non-profit institutions, excluding house purchases.

Financial Risk: Credit Defaults, Liquidity Shortfalls

In any financial transaction, there is always the chance one party may fail to pay the other. Participation in a payment system carries certain responsibilities that are spelled out in Visa's operating rules and procedures. For example, Visa guarantees payment to merchants and the cardholder's bank agrees to transfer payment to the merchant's bank. When a bank cannot meet that obligation (ie, defaults), this not only has a financial impact on the parties, but also threatens to erode confidence in the payment system as a whole. Financial regulators manage a significant portion of this risk through capital requirements and oversight. But private sector networks must provide an added layer of risk management to ensure all parties can meet their obligations.

Criminal Risk: Fraud

Fraud is a classic "moving target". As companies like Visa employ newer and more advanced security barriers, criminals look for new ways to exploit the system. Visa is committed to constant vigilance and the deployment of the latest technology to ensure it will always stay ahead of fraud.

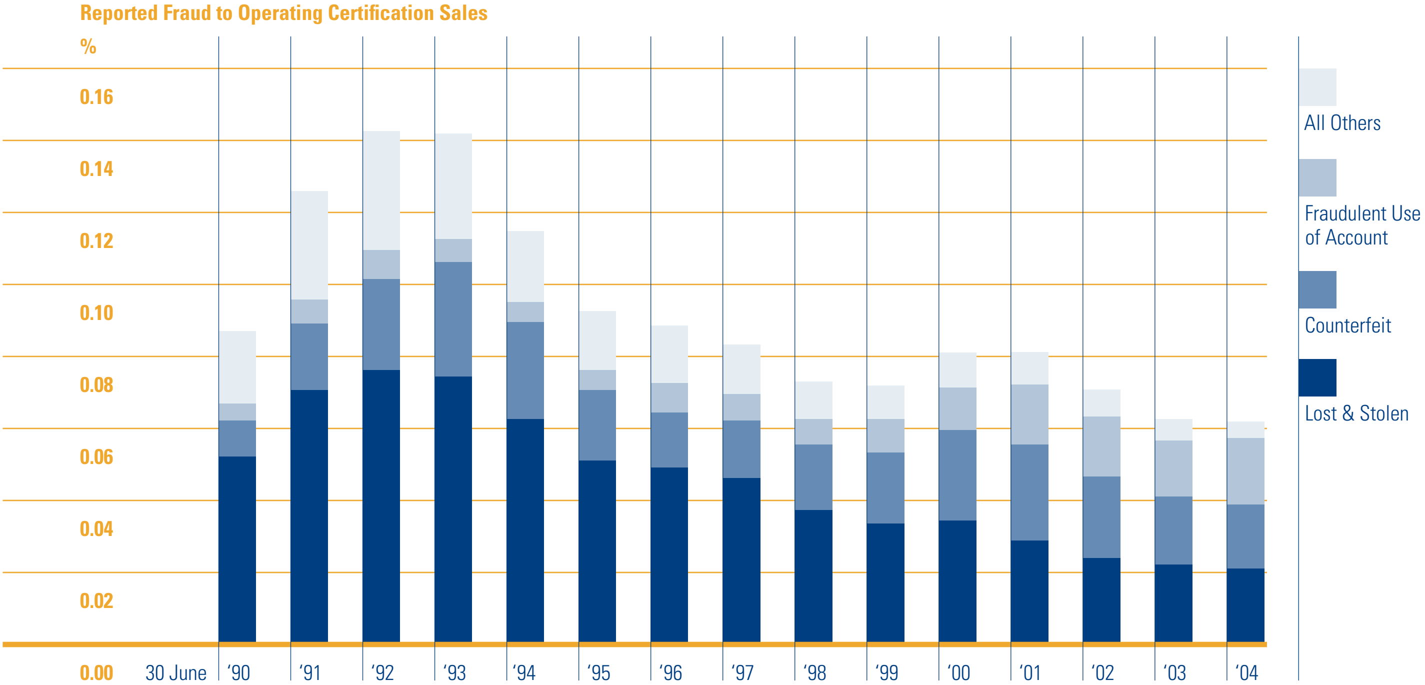
Visa has systems in place to address all types of risk; however, this paper focuses on the prevention and reduction of fraud within retail, electronic, card-based transactions.[2]

[2] For a more detailed explanation and examples of transactions in a retail electronic payment system, like Visa, see the Commonwealth Business Council and Visa International, "Payment Solutions for Modernising Economies", (September 2004), pp. 4–9.

Figure 2

Visa Global Fraud Trends by Type: 1990–2004

Source: Visa International



It is important to understand that Visa and its member financial institutions will never send an e-mail asking for confidential information such as account numbers, passwords, PINs, credit card numbers or Social Security numbers. Consumers should protect themselves against fraudulent e-mails claiming to be from credit card companies, banks or other popular internet websites.

Fraud Types and Trends

To grasp the complexity involved in driving fraud out of a retail payment system, it is helpful to understand the types and nature of the most prevalent forms of fraud. Historically, the most common type of payment card fraud involves lost and stolen cards. As Figure 2 shows, lost or stolen credit cards accounted for more than half the total credit card fraud in 1993. Today it represents a smaller percentage due in large part because of the many security programmes, procedures and management techniques that have been implemented.

The second largest share of fraud is from counterfeit and altered credit cards—ie, those illegally manufactured by individuals or organised crime rings. Generally, counterfeiters use a process called "skimming", where the information contained on the magnetic stripes of valid accounts is technologically lifted and inserted on phoney cards, which are then used to make fraudulent purchases.

The third category of fraud, known as "fraudulent use of account", is a particular risk in card-not-present environments such as ordering by phone (known as Mail Order Telephone Order or MOTO) and e-commerce over the internet. Here, criminals transmit stolen or compromised cardholder information to make purchases without physically presenting a card for authentication by the seller.

A final category includes impersonating a creditworthy person in order to get a credit card or intercepting a card in the mail before it reaches the valid cardholder.

The transaction flow itself also presents a number of opportunities for criminals to obtain information—primarily cardholder data—that can be used to commit fraud. These "touch points" include point-of-sale terminals, telecommunications lines, the internet, telephone orders, wireless networks and ATMs, all of which must be secured.

One relatively new technique that people should be aware of is called "phishing". In phishing, the criminal poses as either the legitimate card issuer, the cardholder's own bank or a seller where the cardholder has recently made purchases. The criminal solicits, often by e-mail, personal financial data and other account-related information such as passwords. TowerGroup estimates that direct fraud losses attributable to phishing amounted to $137.1 million globally in 2004. That number is far below widely cited levels of $1 billion or more and is just a fraction of the total fraud encountered by financial institutions.[3] Phishing, once an issue primarily in the North American markets, is now migrating to other countries and is occurring in other markets with robust e-commerce sectors.

Phishing for Information

When Morita Masatoshi received an e-mail claiming to be from Visa but asking for his cardholder information, he thought it appeared "phishy". He was not alone, as a number of cardholders in Japan had received similar e-mails. This was in November 2004 and it was the first phishing incident in the country, and the suspicious cardholders notified Visa. Quick to react, Visa worked with government officials and law enforcement agencies and helped form a cross-industry anti-phishing working group to share information, educate consumers and raise awareness about phishing. Visa's strong commitment to the prevention and detection of phishing fraud at a global level means the bogus sites are shut down quickly.

The growing incidence of phishing shows some similarities to the rise in telemarketing fraud that occurred in the 1990s when card-not-present transactions were first allowed. Now, as then, the most critical component to protecting cardholders is consumer awareness. Whether it is via the internet or telephone, consumers should never divulge account information unless they were the ones to initiate contact.

[3] "A Phish Story", by Michael Sisk, Bank Technology News, January 2004.

Reliability: Securing the Baseline

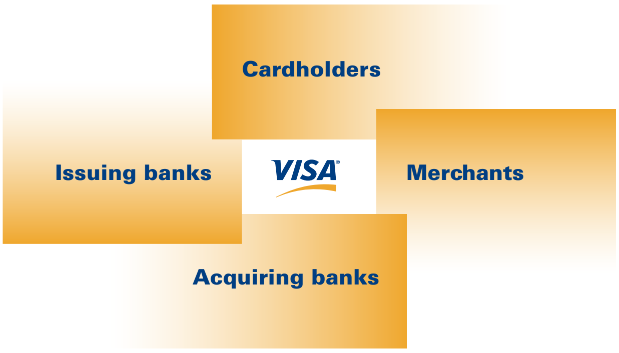
Visa has built its business on a principle that may seem counterintuitive in theory, but works quite well in practice: competitive collaboration.

Under this approach, companies compete vigorously based on products and services, while sharing and standardising the basic payment service infrastructure. While Visa has pioneered most of the significant developments in fraud management, this has often been done collaboratively to ensure that all parties benefit from improved security. For example, Visa collaborated with MasterCard to create a single set of worldwide requirements, called the Payment Card Industry (PCI) Data Security Standard, for consumer data protection across the entire payments industry. This type of competitive collaboration enables as many participants as possible to offer their services to buyers and sellers. It makes basic transactions more efficient and helps make the entire electronic payment system more secure.

Figure 3

Four-Party Business Model

Source: Visa International



The Visa association itself is an excellent example of competitive collaboration. While its member financial institutions are fierce competitors, they also collaborate to form the largest private sector payment system in the world.

Visa's share of total global consumer payments, as measured by Personal Consumption Expenditure (PCE), has continued to rise, from less than 3% in 1994 to almost 9% in 2004. Visa's projections indicate its share of total global consumption may reach 12% by 2010.

Visa's success is based on four core factors:

- **Organisation.** Visa is a privately-owned, joint-venture association of participating member financial institutions. Members invest in a common set of rules, procedures, technologies and infrastructure platforms that operate globally, yet can be localised to meet the needs of specific markets.
- **Global collaboration.** Visa brings synergy and scale to optimise the efficiency of global commerce. Visa's standards and platforms are essential to connecting buyers and sellers around the world.
- **Reinvestment.** Revenues generated by the system are reinvested in improving the security and efficiency of the system and in new products and services.
- **Culture.** Based on co-operation, self-regulation and a common business orientation, Visa's culture delivers maximum value to each participant in the payment system. Fostering competition among member banks has been essential to the success of the Visa system. Members differentiate themselves by individually choosing what products and services they offer in the market and how they market and price those offerings.

Ultimately, Visa recognises it must constantly earn the trust of buyers and sellers so that it can manage all the risks of an international payment system. Therefore, as a baseline, Visa has the following capabilities in place:

Fail-Safe Network

VisaNet is the global transaction processing network that delivers Visa's promise of secure, reliable payments—anywhere, anytime, any way. Reliability is the hallmark of this system, the largest and most sophisticated consumer financial transaction processing system in the world. Indeed, VisaNet has an unparalleled reliability rate of more than 99.999% over the past ten years. VisaNet can settle nearly 100 million transactions in a single day. During the holiday shopping season in December 2004, the system reached a rate of more than 5,500 authorisation messages per second. And each of these transactions pass through the industry's most sophisticated fraud prevention and detection system.

VisaNet is designed to meet virtually any contingency. Its back-up systems, including power supplies, network connections, hardware, applications and data storage, as well as business continuity plans, are constantly rehearsed, assessed and updated. In addition, many of Visa's solutions to counter and prevent fraudulent activity run on VisaNet.

Checks and Balances

Visa's four-party business model itself contains some of the best protection of cardholder information (Figure 3). Checks and balances are built into the system that connects all of the four parties. To maintain the security of customer data across this process, no single stakeholder has total access to all information. For example, while Visa clears and settles transactions, it typically does not maintain personal information that can track individual spending, such as cardholder name, address, Social Security number or other personal information. The issuing bank holds this personal account data.

It is essential for a payment system to have clear roles and responsibilities for all stakeholders:

- *Cardholders:* A cardholder must use the payment card in accordance with the terms and conditions of use as set out in the cardholder agreement signed with the issuing bank.
- *Merchants:* A merchant must accept payment products in accordance with the terms of the merchant agreement signed with its acquiring bank. The merchant must submit those transactions for clearing in a timely manner and must take steps to minimise the potential for fraud.
- *Issuing banks:* The issuing bank must agree to abide by the payment system's operating regulations in relation to card production, card personalisation, and card account management—including fraud control and risk management—and the timely settlement of all transactions effected by its cardholders.
- *Acquiring banks:* The acquirer must agree to abide by the system's operating regulations in relation to merchant recruitment, merchant account management, fraud control, risk management, and the clearing of all transactions.
- *Payment system:* Visa has performance obligations in terms of the speed and reliability of transaction processing, switching, clearing and settlement on behalf of its member financial institutions. Its activities are overseen by an international board and regional boards composed of these members, to ensure quality of operation throughout the system.

Collaboration: Staying One Step Ahead

Visa never stands still and is always exploring innovative ways to make electronic payments more secure.

Because criminals are always exploring new ways to exploit a payment system, Visa works hard to stay ahead of fraudsters. Over the past decade, Visa and its members have invested in programmes, procedures and management techniques that have significantly reduced the fraudulent use of payment cards on a global basis. These efforts are paying off. Today, fraud represents less than one-tenth of 1% (0.07%) of total Visa card volume compared with a larger percentage (0.14%) in the early 1990s.

Visa has not worked alone in this important effort. It has teamed with other payment programmes, law enforcement agencies and technology leaders to secure the core technologies of the payment system from tampering or intrusion; verify proper identification and monitor all parties to a transaction; follow secure procedures for processing payment transactions; and develop programmes, techniques and technologies for detecting fraud and catching the people who try to commit it.

Visa is particularly proud of its efforts in four areas:

- Visa's proactive, **early warning systems** that identify potential fraud by comparing a transaction to a customer's typical spending pattern
- Visa's **security programmes** and systems that have contributed to the explosive growth in e-commerce and other card-not-present purchases
- Visa's **collaborative work** with members, legislators, regulators, non-governmental organisations (NGOs), law enforcement and consumer groups around the world to raise awareness about fraud and how to protect against it
- Visa's use of **emerging technology** through strategic global alliances and investments with key emerging technology companies in order to stay current with the latest developments in security technology

Fraud Management and Reduction Tools

Visa and its members have taken aggressive steps to help identify potential fraud and security breaches before they happen, and then prevent them. Visa has developed a rigorous set of tools and programmes to achieve this goal.

Neural Networks and Advanced Authorisation Service

With every transaction, another chapter is written in the history of how people shop. Visa has created sophisticated computer models to write that history, keep it current and use it to help predict future behaviour. Because these models continue to "learn" by constantly analysing large amounts of data, they are known as neural networks.[4]

Visa's models, which have access to worldwide authorisation data,[5] have created a neural network that allows members to identify and respond to attempted fraud, often stopping the illegal activity as it is taking place. These neural networks are powerful software tools that can monitor and score purchase transactions by comparing them to thousands of previous transactions. Based on this history, the Visa neural network has extremely powerful predictive capabilities that can identify suspicious transactions as they enter the payment system through the authorisation process. This system enables card issuer banks and sellers to be warned about a potentially fraudulent purchase as it is taking place.

Stopping Fraud in Its Tracks

During an afternoon of shopping at a local mall, a typical shopper, Elizabeth Grant, made several purchases using her Visa card at a major department store. Moving on to a smaller shop, she was about to pay for her next purchase when she realised to her horror that her Visa card was missing. Retracing her steps, she was unable to locate the card. So she got Visa's toll-free number and reported her card as lost or stolen. The Visa customer service agent confirmed her last purchases, told her she would not be responsible for any additional charges and arranged to send her a new card right away. Behind the scenes, Visa was working quickly to prevent fraudulent use of Elizabeth's card by placing a "block" on it. Almost at once, the Visa system received a real-time authorisation request on the card from a jewellery store in the same mall. Someone was trying to use Elizabeth's card to buy an expensive bracelet. But, thanks to the "block", the jewellery store clerk got a "referral" or decline message on her terminal. This enabled her to delay the sale and call police. The surprised thief was arrested while still in the store.

[4] For more information on neural networks and their developments, see "Neural Networks for Pattern Recognition" (November 1995) by Christopher M. Bishop.

[5] Authorisation data does not typically include cardholder information.

Card Activation and Alternative Delivery Programmes

Visa wants to ensure the person who has the card is, in fact, the valid cardholder. Card activation requires the cardholder to take steps to verify they actually have the card in their possession. Usually this involves making a phone call from their home phone number in order for the card to be activated prior to use. To prevent cards from being stolen in the mail, alternate delivery methods are often used in high-risk areas that might pose a particular problem. These relatively simple but important steps have helped reduce fraud by people attempting to steal cards in the mail.

Card Verification Value

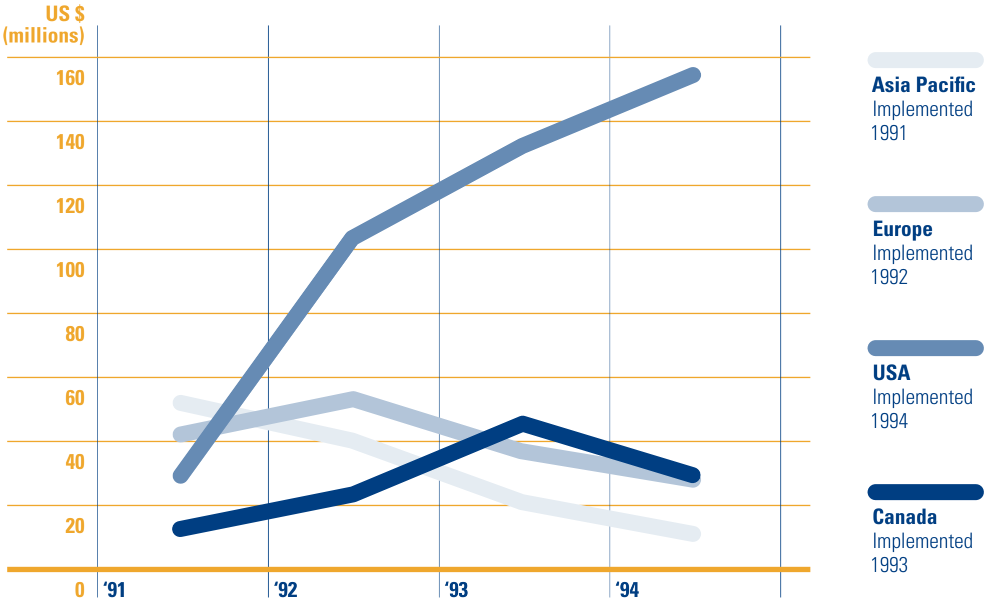
Card Verification Value (CVV) is a risk management tool developed by Visa to thwart counterfeit fraud, such as account generation. It validates that a card account number is legitimate by comparing data stored on the magnetic stripe to that held by the issuer. This control is used to address non-skimmed counterfeit in a face-to-face environment.

As shown in Figure 4, the first adopters of CVV proved very effective in reducing basic counterfeit fraud by as much as 80% compared with later adopters who continued to rely on non-CVV transactions.

Figure 4

Card Verification Value (CVV) Adoption

Source: Visa International



Enhanced Card Verification Value

The Card Verification Value 2 (CVV2) code is an important layer of security to help reduce fraud in so-called card-not-present transactions, like phone, internet or mail order. Introduced in the late 1990s, CVV2 is a three-digit code printed on the back of each Visa card. By asking for the CVV2 at the time of sale, the merchant can be sure the customer actually has the card in hand. As well as reducing fraud, this greatly reduces "chargebacks" that result when people find unauthorised items charged to their Visa account.

As shown in Figure 5, not only does the presence of a match reduce fraud by more than 80%—protecting both merchants and cardholders from fraud—it also increases the approval rate of legitimate transactions. Thus reinforcing the observation that when people trust the security of the transaction, sales improve and healthy commercial trade is supported to everyone's benefit.

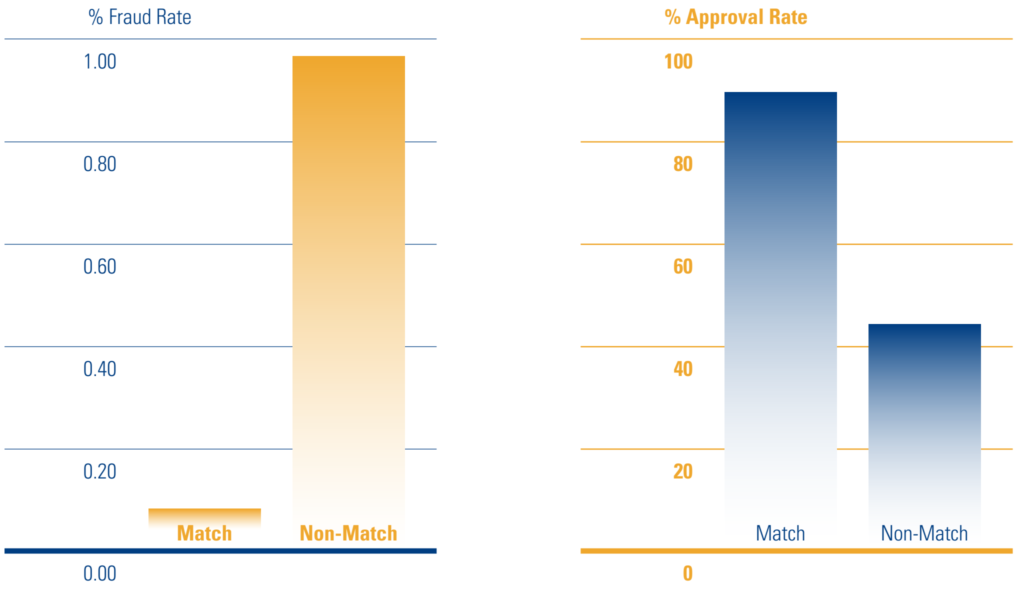
Address Verification Service

Address verification service is available in some markets and is designed to further assist major catalogue and mail order retailers prevent fraud in card-not-present transactions. This service, known by the initials AVS, compares every transaction against the issuing bank's record that contains the buyer's card account billing address and zip/postal code. The retailer and Visa make sure the information provided by the buyer matches the address the issuing bank has on file, returning an AVS code if there is a match. Although the processing network will not reject a transaction based on an AVS response, the code indicating match or mismatch can let the seller decide whether to go forward with the sale.

Figure 5

Card Verification Value 2 (CVV2) Match / Non-Match Fraud Reduction

Source: Visa International



Data Security Programmes

Visa recently announced collaboration efforts with MasterCard and other payment organisations to create a single set of worldwide requirements, called the Payment Card Industry (PCI) Data Security Standard, for consumer data protection across the entire industry. This standard aligns multiple industry programmes and streamlines requirements, compliance criteria and validation processes.[6] It also addresses merchants' and acquirers' concerns about having to meet more than one set of standards to accomplish a single goal.

Visa's PCI programmes outline basic security standards all merchants in the Visa system are required to meet to maintain the confidentiality, integrity and availability of this information. Securing data makes good business sense, and meeting these standards helps merchants build consumer trust, protect the integrity of their own brand and reduce customer disputes.

The standards cover a number of key functional areas, including the protection of sensitive cardholder data on websites, servers and stand-alone computers. It provides an assessment of a merchant's existing security practices benchmarked against "best in class" practices for securing cardholder transaction and account data, including access to data, firewall integrity, encryption of stored data and physical security. Visa's data security programme served as the model for best practices published by the G-8 at its 2001 Conference on High-Tech Crime in Tokyo and was the first set of standards within the payments industry for online data security.

Cardholder Account Number Truncation

During 2003, Visa USA required that all point-of-sale and virtual sellers implement cardholder account number truncation to combat identity theft. Under this programme, Visa limits—or automatically truncates—the cardholder account numbers shown on receipts to include only four digits and eliminates the card's expiration date from receipts altogether. This added security feature protects the buyer's identity by restricting access to account information on receipts that could be lost or stolen. In Visa Europe, this mandate will be in force by July 2005, although many merchants have already modified their equipment.

Change Warnings from Tripwire

Payment systems need to know about changes in data. Is the change authorised? Can we account for it? Or is it the result of an inadvertent error or an outside hacker? These common questions arise when changes in financial data are identified. Two years ago, Visa entered a strategic partnership with Tripwire, Inc. to explore the application of the company's data change detection and reporting technology to the financial services industry. At present, Tripwire continues to be one of the premier vendors for Visa data security compliance, and their award-winning products and technology align with Visa's goal of making electronic payments safe and secure, whether they take place over the internet or at the point-of-sale. Tripwire currently works with a wide variety of Visa merchants and service providers to help them comply with the Visa guidelines necessary to become certified. Overall, Tripwire helps create a safe, productive and stable IT environment, and provides an extra layer of security for member banks, merchants and consumers worldwide by helping to ensure the integrity of financial data.

[6] Visa's Account Information Security (AIS) programme is designed to help merchants in both the physical and virtual worlds protect sensitive account and transaction information. Visa has implemented this programme in Asia Pacific, Canada, Europe, Latin America and the Caribbean, and in the United States under the name Cardholder Information Security Programme (CISP).

Smart Card Technology

Smart cards are the future of electronic payments. Featuring an embedded microchip, they offer consumers more options, more services, more convenience and greater security than traditional magnetic stripe cards.

Without a doubt, the magnetic stripe was a breakthrough for its time. Encoded with basic cardholder information, the stripe helped secure transactions at the point of sale.[7] Smart cards have greater capability. They can be encrypted with debit, credit and prepaid applications, be personalised with individual spending limits, and are useful in countries that do not have the well-developed land-based telecommunications system needed for rapid authentication.

In countries where smart card use is widespread, there has been a significant reduction in fraud. When used with a personal identification number (PIN), smart cards have cut fraud from lost or stolen cards by 90%. And, because the computer chip can be upgraded, new levels of security can be added to combat fraudulent activities when necessary.

Before smart cards can fulfil their potential, global standards have to be created so Visa cards can continue to be accepted everywhere, a requirement known as interoperability. Visa was instrumental in obtaining agreement on common standards and a framework for a seven-year European migration to the EMV[8] standard for all payment cards. Visa Europe provided a chip migration fund of approximately US$190 million to support members, sellers and vendors in their efforts to transition to smart cards. In addition, by 2008, these efforts will result in full implementation of smart card technology throughout the Asia Pacific Region and by 2010, almost every Visa card in Canada will feature chip technology. Furthermore, Visa continues to drive the standards for utilising the enhanced technology on chips beyond these initial security features for multi-application purposes, like GlobalPlatform. In combination, these standards and open platforms have enabled issuers to offer smart cards that utilise various features and technology in a cost-effective manner. As a result, the price for a basic smart card has fallen from around US$8 per card in the late 1990s to less than a dollar today.

[7] Additional card security features to avoid counterfeit include the raised embossing of the account number, name and expiration date on the face of the card, the size and placement of various logos and embossments, additional printed numbers, and, for authentication purposes, the signature panel and printing of the account number on the back of the card. While pictures on cards have been supported by Visa and promoted by various card issuers as a potential card authentication security feature, such pictures have typically been used more from a marketing perspective to differentiate issuing bank product offerings and as a potential tool to retain customers.

[8] EMV: Europay, MasterCard and Visa.

Visa has worked with other international payment systems, industry groups and technology leaders to create these standards, including EMV. This standard ensures the acceptance of smart cards at point-of-sale terminals and ATMs around the world. It is helping to speed the world's transition to this newer, more secure card technology. Visa is also driving the standards by which microchips can be used for a variety of new applications. GlobalPlatform, created by Visa, allows issuing members to provide marketing and other information on the card.

The Smart Solution to Fraud

The United Kingdom is leading the world into the EMV age, with more than half of the country's Visa cards carrying an EMV chip. Its business case is based firmly on fraud control—and its strategy is working. National losses on all counterfeit cards fell from US$231 million in 2001 to US$214 in 2002 and the country's Association of Payment Clearing Services believes that criminals are actively avoiding chip cards and terminals. A Visa study underlines the trend, showing that, even before the infrastructure upgrade was complete, domestic counterfeit fraud among issuers who had upgraded most of their cards to EMV chip was 43% lower than among similar banks who still issued magnetic stripe cards. Cross-border counterfeit was 38% lower. The introduction of chip and PIN is expected to drive down losses even further—the European Commission estimates that it will lead to savings of US$706 million a year when it is implemented across Europe.

Securing E-Commerce

Visa is committed to bringing the same level of convenience, acceptance and security to the virtual world as it has to the physical world. Today, cards are the preferred payment type for e-commerce buyers and sellers around the world.[9] But there are still challenges to address. According to Celent Communications, online merchants have experienced fraud rates that are 30 times higher than their US brick-and-mortar counterparts.[10] And studies indicate many potential buyers have security concerns that keep them from using payment cards on the internet. For example, several surveys show card security as the number one reason why buyers do not make online purchases.[11] And in a recent survey conducted among internet buyers in the United Kingdom, nearly 75% claimed data and information security was more important than price, quality or convenience when shopping online, while 70% indicated they would boycott a website even if they only had word of mouth evidence the site or seller had been involved in a security breach.[12] In addition, merchants have concerns about protecting their reputation, customer relationships and bottom lines when a legitimate customer's payment account is used illegally.

To realise the full potential of e-commerce, Visa is taking steps to increase confidence in online payment security so buyers and sellers understand that the payment system will (1) facilitate an efficient, convenient and error-free exchange of money for products or services, and (2) protect the security of data exchanged during each transaction.

Verified by Visa Programme
Verified by Visa is a critical tool in reducing the potential for internet fraud and increasing consumer confidence in shopping online. With Visa's overall fraud rate half of what it was six years ago, Verified by Visa is expected to reduce internet transaction disputes by at least 50%.

When cardholders sign up for Verified by Visa with their bank, they receive a personalised password. As they shop online, they enter the password during the check-out process, confirming they are, in fact, the cardholder authorising the sale. The programme has several important advantages that are critical to the growth of e-commerce. It gives the cardholder more control over when and how their card is used and it relieves the merchant of liability for chargebacks when there is a dispute over authorisation. E-commerce transactions are much more likely to be disputed and charged back than transactions that take place face to face. And 80% of all chargebacks occur when the cardholder says, "I didn't buy that."

[9] Nilson Report #740/May 2001 and #750/October 2001.

[10] Celent Communications, "Taking a Bite out of Credit Card Fraud", by Ariana-Michele Moore, January 2003.

[11] "Consumer Concerns Over Identity Theft and Fraud", by Kate Delhagen, Forrester Research, June 21st 2004.

[12] See results of a survey conducted by Tickbox.net, an online research company, for LogicaCMG, July 8th 2004.

As noted in Figure 6, since Verified by Visa was implemented in 2003, there has been a 75% reduction in chargebacks on Verified by Visa compared with non-Verified by Visa transactions.

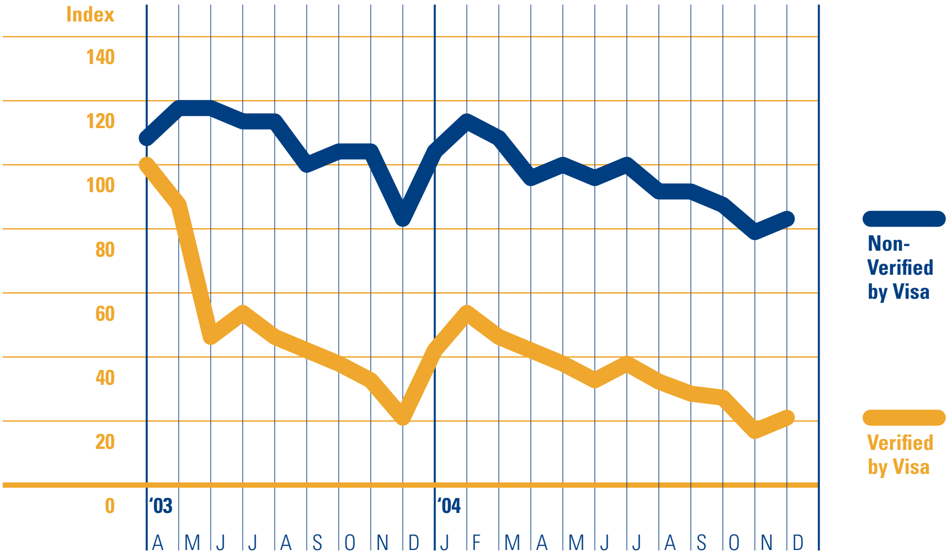
The Verified by Visa programme uses Secure Sockets Layer (SSL) encryption technology. It also uses a suite of proprietary fraud detection and management services that protects the exchange of transaction information among sellers, buyers and banks. Verified by Visa has received numerous industry recognitions and awards, including the 2004 Lafferty Technology Award.

By advocating adoption of the Verified by Visa programme, internet service providers, processors and independent sales organisations are also able to strengthen their relationships with internet sellers by offering a value-added service that can generate additional sales revenues. As a result, internet sellers around the world are seeing the tremendous importance of adding Verified by Visa to their websites.

Figure 6

Verified by Visa Chargeback Comparison

Source: Visa International (December 2004)



Global adoption of Verified by Visa is accelerating, with implementation in more than 65 countries representing 99% of global e-commerce volume. More than 10,000 Visa members now offer the service, thus making it available to more than 355 million debit and credit cardholders worldwide. These cardholders can shop safely knowing their account information is protected from misuse at more than 30,000 internet sellers, and that the rate of internet seller acceptance continues to grow rapidly.

Recently, Visa added an additional optional layer of technology to the Verified by Visa programme. The Dynamic Passcode Authentication programme combines smart card technology, the cardholder's PIN and a calculator-sized card reader the cardholder obtains for their home. When the card is read during each online transaction, it displays a one-time-only passcode that is used to authenticate the online sale. This raises the bar against fraud by ensuring only the cardholder is able to use the card.

Global adoption of Verified by Visa requires an ongoing education effort aimed at raising public awareness. As the security protocol is introduced into new markets and consumer adoption spreads, would-be criminals will likely be driven out of business, making the Visa shopping experience even safer and more gratifying.

Partnerships and Emerging Technologies

Visa forms partnerships with key emerging technology companies to build the next generation of secure global commerce and payment infrastructure in the financial services industry. Innovative solutions from partner companies also play a role in strengthening the Visa brand in the global market, enhancing relationships with members and merchants, and delivering new levels of security, trust, value and productivity.

Partner companies help Visa deliver on its promise to deploy and maintain an infrastructure that is safe, secure and compliant with all applicable security regulations. These companies span the breadth of the security industry, offering solutions in such areas as intrusion detection, database security, secure authentication, network vulnerability, change control and intelligent content monitoring.

In February 2005 Visa together with Microsoft, eBay and WholeSecurity launched the first global anti-phishing service, the Phish Report Network. This allows any company being victimised by phishing attacks to immediately and securely report fraudulent websites to a central database. Other companies subscribing to the Phish Report Network can then access the database or receive real-time notifications of known phishing sites, enabling them to more effectively protect consumers.

Protecting Against "Insider Threats"

Visa's alliance with Vericept demonstrates how partner companies can help enterprises minimise risk through Intelligent Content Monitoring. Vericept's solutions provide visibility to inappropriate activity across all forms of internet traffic. This includes web, e-mail, chat, instant messaging, bulletin board postings, blogging and Telnet in real-time. Vericept provides the information and the capability to take appropriate action—almost immediately—and prevent losses of valuable information assets such as customer data and internal financing, marketing and research plans. Financial institutions are deploying Vericept solutions to prevent the leakage of credit card information, government identification numbers and other private customer information. Enterprises across a variety of market segments are adding Vericept technology to their layered security solutions to detect inappropriate use of the internet that could result in risk to the company and its employees and customers.

Leadership: Contributing to the Industry

As the global leader in electronic payments, Visa is proud that many of the solutions it has developed have become the industry standard. On matters of payment security, Visa defines success in terms of the security of the electronic payments industry as a whole.

For more than 30 years, Visa has developed technologies and applications to better manage and control fraud. In fact, Visa has an ongoing commitment to strengthening the payment services industry overall. Visa's initiatives to create industry standards for security and fraud control practices, as well as its joint efforts with law enforcement and other payment organisations, are making the "anywhere, anytime, any way" experience a more secure one for the customer and a more profitable one for merchants and Visa's members.

Some of these innovations remain proprietary to Visa, but in many cases these efforts and solutions have been donated to the industry as best practices. As discussed earlier, CVV/CVV2 and chip standards such as EMV and GlobalPlatform are prime examples of Visa's contributions to industry security. In fact, Visa has taken the lead in working with other international payment systems, industry groups and technology leaders to develop global standards and specifications for interoperability so that this technology can reach its full potential. Table 1 highlights the wide range of security innovations and solutions Visa has developed or enhanced since the 1970s.

Table 1

Visa's Fraud Control Innovations and Industry Best Practices

Security Initiative	Evolution / Issues	Time Frame	Region
Card Features	Signature Panel, Embossing, Card Real Estate Design, & Microprint	1970s on	Global
Card Expiration Date (embossed)	Physical Security (MOTO in particular)	1970s on	Global
Risk Identification Service	Evaluates transactions and reports merchant-related fraud	1980s	Global
Issuers Clearinghouse Service	Database for negative file	1980s	US
Magnetic Stripe Technology	Authorisations	Early 1980s	Global
Secured Electronic Clearing & Settlement Network	Network Security of transactions	Early 1980s	Global
Hologram	Physical Security—marketing/public relations initiative	Mid 1980s	Global
Address Verification Service (AVS)	MOTO Security and accompanying AVS code	Late 1980s	US & Europe
Cardholder Risk Identification System (CRIS)	Identify fraudulent transaction patterns	Early 1990s	Global
Card Verification Value (CVV)	Enables Issuers to validate code on card's stripe/secured cryptographic process	Early 1990s	Global
Neural Networks used globally for Advanced Authorisation Service	Identify and adapt to emerging fraud (ex. VISOR - Europe)	Mid 1990s	Global
CVV2	Enables Issuers to validate code on back of card and is in purchasers' hands during a card-absent transaction	Late 1990s	Global
Bankruptcy Prediction Service	Credit Risk Management	Late 1990s	US
Payment Card Industry (PCI) Data Security Standard: Account Information Security (AIS) Cardholder Information Security Programme (CISP)	Enhanced Security protecting data simultaneously in physical and virtual environments	2000	Global
GlobalPlatform	Multiple applications on chip	2000	Global
3-D Secure/Verified by Visa (VbyV)	Safe-guards on-line buyers and sellers by authenticating buyer and their account information	2001	Global
EMV/Chip & PINs	Initial Chip card standard	2003	Global
Truncated Account Numbers	Truncates the full account number on physical receipts to last four digits	2003	US, Canada & Europe (in July 2005)

Card Features and the Hologram

Visa introduced a number of unique card design features and standards that have served two very important purposes: providing ample room for member banks to create customised cards that appeal to their customers, while at the same time protecting the card from counterfeit. Many of the security features on the card reflect unique micro-printing, lamination and card embossing standards. Perhaps the most recognisable feature—and still one of the most secure—is the dove hologram foil technology that was introduced in 1983. The Visa design team created an enhanced method of merging foil and hologram picture technology to reproduce a three-dimensional image of a dove in flight. Licensed to only a few manufacturers in the world, the Visa hologram is easily recognisable by sellers and buyers, and is very difficult to counterfeit. Recently, Visa announced that it will be moving the famous dove hologram from the front of the card to the back and combining it with the magnetic stripe. This move enhances security by creating a holographic magnetic stripe that integrates both overt and covert security features, creating a particularly effective counterfeit-prevention device.

Supersleuth Kits

To help law enforcement agencies join the fight against credit card fraud, Visa is issuing toolkits—fondly known as "supersleuth suitcases"—to police officers in its CEMEA Region (Central and Eastern Europe, Middle East and Africa). Each sturdy aluminium case is packed with tools investigators can use to examine suspect cards and devices: a strong magnifying glass to check card micro-print, a card-reading terminal, a digital camera to record evidence and an ultraviolet light to check card watermarks. The officers also receive a CD-ROM containing training materials so they can learn more about credit card crime and how to stop it.

Fraud Prevention Education

The more buyers and sellers are aware of how fraud can happen, the better they can protect themselves and the easier it is to prevent fraud. Education and increasing awareness therefore are critical. Visa has organised conferences and seminars and provided education materials for schools, libraries, and consumer advocacy and retailer groups. These materials include information on how to protect Visa cards and use them safely, as well as data on emerging trends in payment card fraud, proper card acceptance procedures and payment card security features. In addition, Visa has developed online education on secured transactions as well as making available information on our websites for consumers to detect and prevent fraud.

Visa has also worked with government organisations, providing draft information and testimony before legislative and regulatory bodies, and supporting law enforcement agencies around the world with information to better identify and manage fraud and security on electronic payments.

Visa's efforts have been instrumental in helping reduce payment system fraud in the European Union where it has been reduced by more than 41% over the past ten years.[13] Visa has also been a leader in co-operating with local, national and international law enforcement to ensure their participation in combating fraud.

[13] Visa International statistics from 4QE June 1993 to 4QE June 2004.

Certifying Scottish Experts

In the late 1990s, Visa's Europe region initiated a programme to train and certify Scottish police officers as experts on counterfeiting. This enables them to testify as experts in court. Before that, Visa supplied experts to assist Scottish police and prosecutors in court cases. Today, the Visa certification programme has reduced delays and the costs of prosecuting suspected counterfeiting criminals in the Scottish courts. Most importantly, the prosecution rate in counterfeiting cases has increased.

Seller Security Awareness, Legislative and Regulatory Changes

Globally, organised criminal groups commit a large proportion of fraud, often using sophisticated counterfeiting techniques. These groups endeavour to quickly identify weak links in the payment system—be they geographic areas or participants—and refocus their illegal efforts accordingly. Many criminals take advantage of poorly trained retail clerks and sellers; they also target inexperienced issuer and acquirer banks. Visa and other card-based payment systems have designed many initiatives around the world to help issuers, acquirers, buyers and sellers detect and stop fraudulent activity. These programmes have had great success in several markets, where fraud has sharply declined soon after Visa initiated security-related seminars, legislative initiatives and training programmes. However, as indicated, fraud sometimes migrates to neighbouring markets where these programmes have yet to be introduced or organised.

For that reason, Visa's regions play an important role in developing and introducing measures designed to help specific markets and members. In many Eastern European countries, for example, Visa's CEMEA region has organised forums where members, law enforcement agencies and other institutions can meet to discuss risk-related issues. Fraud on Visa cards in the region has fallen from a high of 0.45% of sales in 1996 to an average of 0.09% in 2003. Visa's efforts have been especially critical in three key markets: Hungary, Romania and Bulgaria.

Working with Merchants

Visa and its members set up a working group in Bulgaria to concentrate on card criminals moving into that country during the Olympic Games in Athens and the summer tourist season. The group installed systems to monitor issuing and acquiring members, and created a centralised database of merchants who were involved in collusive and fraudulent activities. This database prevented fraudulent merchants from signing with a new acquirer bank when their contracts were cancelled. It also enhanced overall merchant compliance with Visa's transaction processing requirements. As a result of these aggressive steps, better communications and the tremendous support of the merchants, acquirer fraud has virtually been stopped in the region.

Conclusion

Visa Solutions: Securing the Future of Electronic Payments

The use of electronic payment products to conduct commerce has grown dramatically over the past 30 years, as buyers and sellers recognise the significant benefits in purchasing goods and services across a wide variety of locations, markets and channels.

Electronic card products and payment systems, like Visa, have been successful because they have provided the necessary flexibility, interoperability, scale, security, convenience, universal acceptance and product features required in the changing global commercial environment. Cash and cheques, by comparison, simply have not been able to keep pace with all of these features, resulting in a relative decline in their use and a growing acceptance of electronic payment products.

The demands of buyers and sellers for efficient, convenient and secure payment systems will continue to grow. As in the past, successful payment systems will be those that respond quickly and lead this evolutionary process through the use of technology, innovation and enhanced security to satisfy those demands. Electronic payments are also certain to be a driving force underlying the future development of efficient financial systems in emerging markets.

Unfortunately, the continued growth and acceptance of electronic payments will also attract the attention of organised crime rings and others seeking to compromise the payment systems through fraudulent activity. Continued investments in security and fraud management technologies must be made to maintain and enhance the security of these systems and to bolster the confidence of buyers and sellers. Furthermore, to be successful, these efforts will have to be reinforced with proper governance, adequate financial security legislation, and mutually agreed upon standards, control mechanisms and processes among various stakeholders.

It took the development of bankcard associations, like Visa, to ignite growth in electronic payments beginning in the 1970s. Collaborative investments and agreements were required in order to achieve the scale necessary to distribute the cards and sign up sellers efficiently and securely. No single player could have justified the investment to create the infrastructure and processes necessary to make the system work. This type of organisation has resulted in a card-based electronic system that has fostered competition among its members while centralising those aspects of the system that jointly benefit all members—especially authorisation, clearing and settlement, and security and risk management. Additionally, the association model allowed the industry to grow and evolve to meet changing market and stakeholder needs based on a common purpose.

Visa's ability to build on collaborative investments in new technologies, processes and programmes has led the way in identifying, managing and reducing security and fraud risk for buyers, sellers and member banks. In combination, these efforts have been the glue that has bound together the buyer and seller relationship that continues to support a much higher level of trust than is possible with any other payment system. As a result, the Visa system has provided the global economy with the payment products and systems that have transformed transactions into commerce.

With Visa's industry-leading risk management programme, the continued pursuit of every possible means of fraud prevention and detection will be a top priority. Ensuring the security and integrity of the payment system is at the heart of Visa's brand promise.

Glossary

Account Generation – A type of fraud where a computer program, sometimes found on internet sites, is used to generate card numbers. Fraudsters may then use these numbers in card-not-present transactions to test if they have a "live" account number. If they do, they may use that number to then generate other numbers to conduct additional card-not-present transactions before the fraudulent use is detected.

Account Information Security (AIS) – Defines the basic security standards for merchants to protect cardholder information.

Acquirer – A member financial institution that supports and enables merchants to accept Visa cards for payment. Many members perform both issuing and acquiring functions.

Automated Clearing House (ACH) – A regional organisation used to electronically transfer funds between members.

Address Verification Service (AVS) – AVS helps mail order and catalogue merchants reduce risk associated with these card–not–present transactions. AVS verifies the billing address given by the buyer matches the billing address on file with the buyer's credit card issuer.

Authorisation – A process, as specified in the Visa Operating Regulations, where an issuer, an authorising processor or stand-in processor approves a transaction.

Buyer – The person to whom a financial transaction card is issued or an additional person authorised to use the card.

Card-Not-Present (CNP) Transactions – Credit or debit card transactions that take place over the phone, through the mail or on the internet.

Card-Absent Environment – Transactions that do not take place face to face. In these transactions, neither the cardholder nor the card is present. Transactions in this environment include mail or phone order, recurring transactions and telephone service transactions.

Card-Present Environment – Transactions that take place face to face or at a cardholder-activated terminal.

Card Verification Service – A VisaNet service where Visa validates account information stored on the card with information maintained by the issuing bank.

Card Verification Value (CVV) – A unique value encoded on the magnetic stripe of a payment card to validate card information during the authorisation process. CVV is calculated from the data encoded on the magnetic stripe using a secure cryptographic process.

Card Verification Value Programme – A Visa programme that enables issuers to validate the Card Verification Value, ensuring that it matches the value encoded at the time of issuance.

Card Verification Value 2 (CVV2) – A unique three-digit code printed on the back of each Visa card. By requesting this number at the time of a card-not-present sale, the merchant can be sure the buyer is in possession of the card.

Chargeback – A disputed transaction initiated by the consumer's card issuer at the request of the consumer after settlement of the transaction by the merchant. If the consumer wins the dispute, the amount is refunded to the consumer and charged against the merchant's settlement account.

Chip Cards – Cards with an embedded microchip, also referred to as "smart cards". Chip cards are inserted into a terminal instead of swiped like a magnetic stripe card. Considered the future of electronic payments, smart cards have greater capability than magnetic stripe cards to contain additional applications and information.

Counterfeit Card – There are several basic types of counterfeit cards. First, a card can be printed, embossed or encoded to look like a Visa product when it is not. Second, a Visa product may be produced with the authority of an issuing bank but is later embossed or encoded without the bank's authority. Third, a Visa product that is changed or altered illegally.

E-Commerce – Doing business via the internet, either from a merchant company's website or by using a Virtual Terminal.

Electronic Payment – An electronically processed payment not using cash, currency or paper-based systems, like cheques.

Electronic Payment System – A processing, clearing and settlement system that forms the basis of all electronic payment networks.

Embossing – The process of printing data, in the form of raised characters, on the bankcard that provides identification of the card and allows the imprinting of sales drafts at point of sale.

Floor Limit – A monetary amount set by the acquirer in accordance with Visa rules and regulations. The merchant must obtain authorisation for any transaction over the floor limit.

Fraud Activity – Either a transaction where the cardholder did not authorise or take part in the transaction, or a case where someone misrepresents their identity or financial status to the issuing bank in order to obtain a Visa account.

Fraud Advice – A VisaNet transaction through which an issuer may report fraud activity.

Hologram – A laser-created photograph that creates a three-dimensional image; used as an anti-counterfeiting measure on bank cards.

Identity Theft – Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes.

Issuer – The financial institution that issues the customer a credit card and settles with the merchant bank when the customer charges something on their Visa card. The issuer will then bill the transactions to the customer's account/statement. Visa does not issue payment cards.

Magnetic Stripe – The magnetic stripe is on the back of a card and contains encoded card account and other data.

MOTO – Short for mail order (MO) or telephone order (TO).

Online – A method of requesting an authorisation through a communications network, other than voice, to either an issuer or an authorising processor.

Payment Cards – A card-based payment product issued based on a line of credit (charge or revolving credit), fund on deposit (debit), or cash value that has been deposited into an account (prepaid). Payment cards utilise the card payment infrastructure such as point of sale, internet-based person-to-person or business-to-business systems, mobile phones and/or bill payment systems.

Payment Card Industry (PCI) Data Security Standard – Visa recently announced collaboration efforts with MasterCard and other payment organisations to create a single set of worldwide requirements for consumer data protection across the entire industry. This standard aligns both AIS and CISP programmes, streamlining requirements, compliance criteria and validation processes. It also addresses merchants' and acquirers' concerns about having to meet more than one set of standards to accomplish a single goal.

PIN – A personal identification alpha or numeric code that identifies a cardholder in an authorisation request originating at a terminal with electronic capability.

PIN Verification – A procedure used to verify cardholder identity when a PIN is used in an authorisation request.

Phishing – A fraudulent spam e-mail and/or website disguised as a trusted brand intended to trick consumers into divulging personal and financial information, which is later used for identity and financial theft.

Sales Draft – A paper record showing the cardholder's purchase of goods or services from a merchant using a Visa product.

Skimming – A process counterfeiters use to technologically lift valid account information contained on the magnetic stripes and insert into phoney cards, which are then used to make fraudulent purchases.

Secure Sockets Layer (SSL) – A security standard that many merchants use to keep their websites secure and to protect the safety, privacy, and reliability of payment data travelling over the internet. SSL encrypts the channel between browser and Web server so only the intended parties can read certain data, such as payment or customer information.

Verified by Visa – Visa's global payment authentication programme that enables consumers to add their own personalised password to their existing Visa card. As they shop online, consumers use this password to verify their identity in real-time to their issuing bank before the sale is completed. Designed to closely replicate a "card present" environment, Verified by Visa reduces the risk of fraud and chargeback costs, with minimal impact to the merchant's current transaction process.

Zero Liability – Visa's policy that eliminates consumer liability in case their card is used fraudulently to charge transactions, including online transactions, through the Visa network (available in the US and Canada only).

Notes

For additional information, contact Visa International Global Corporate Relations: globalmedia@visa.com or www.corporate.visa.com

Visa International
P.O. Box 8999
San Francisco, California 94128