Visa's Security Agenda for Southeast Asia

Contents

For more information please visit:
www.visa-asia.com/secured
www.visasecuritysense.com

Introduction

Ensuring Visa transactions are secure is one of our highest priorities. That's why we have invested millions of dollars in security and with every payment innovation we make, we ensure security remains the number one consideration.

Times are changing and so is our payments system. Consumers have never enjoyed more choice in the way they can make payments in-store, online, over the phone, both domestically and overseas.

At Visa we've been working hard to provide our cardholders with more convenient, efficient, simple and secure payment options.

With this firmly in mind, I'm pleased to launch Visa's Southeast Asia Security Agenda which demonstrates how Visa is working in collaboration with banks and merchants to strengthen the payments system across Southeast Asia.

In order to strengthen the payments system, we have developed a strategy that is based on five key pillars:

- **Adopt EMV chip for cards**
  Securing the cards
- **Deploy EMV enabled acceptance devices (POS, ATMs)**
  Securing the acceptance environment
- **Verified by Visa for cards supporting One-Time Passcodes**
  Securing the online environment
- **Robust fraud detection capabilities**
  Providing real time risk intelligence on transactions occurring at retail POS, online or ATMs
- **Payment Card Industry (PCI) Data Security Standards (DSS)**
  Educating merchants and third party agents on data security and compliance to the standards

We will be working with the industry to reach alignment on these initiatives, to ensure that Southeast Asia's payments system remains among the safest in the world.

Ooi Huey Tyng
Country Manager for Singapore and Brunei
Visa

"Visa's approach to security is based on the belief that the only effective way to protect our cardholders, clients and merchants, is to employ multiple layers of security."

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 make unauthorized transactions.

The criminals of today - 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 to security is based on the belief that the only effective way to protect our cardholders, clients and merchants, is to employ multiple layers of security. Simply put, there is no "silver bullet".

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 unauthorized transactions, 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 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.

Payment Security Concerns

There are three major types of payment card security concerns – counterfeit, unauthorized usage in card-not-present environment, and misuse of lost and stolen cards. In addition, hacking and phishing are two of the common methods criminals use to obtain cardholder information to commit unauthorized transactions.

Counterfeit

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

This type of security threat is committed without the actual use of a card - for instance in online or over the phone transactions. We have seen card-not-present security threats increase in recent times due to growth in eCommerce and as the roll-out of chip cards and terminals has made it more difficult for fraudsters to compromise the point of sale. Criminals like the card-not-present environment because they do not have to be physically present to commit the crime.

Lost and stolen cards

This activity 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 transactions or to make counterfeit cards.

Phishing

Criminals looking to gather financial information have developed a way to lure in suspecting 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 unauthorized transactions.

ATM skimming

In recent years, in response to various business needs such as risk concerns relating to counterfeit cards, clients in a growing number of countries have chosen to adopt EMV chip technology. To accelerate the deployment of EMV chip technology, most Visa regions either revised their domestic and intraregional rules or approved new rules to address security threats that might have been prevented if EMV chip technology had been used by both parties in a transaction. These rule changes shift the liability from issuers that have invested in chip technology to acquirers that have not invested in EMV chip technology.

Electronic pickpocketing

Some TV news reports have tried to demonstrate a scam known as electronic pickpocketing whereby a fraudster uses a scanner to steal information from a contactless card, unbeknown to the cardholder. The cardholder is then advised to use protective covers to protect their cards and passports when they're not in use.

The potential security risk from this type of scam is limited because of the multiple layers of security that protect each Visa transaction. In fact, there have been no reports of unauthorized transactions perpetrated by reading Visa payWave cards as demonstrated in these reports.

While companies selling protective card covers potentially have a financial incentive to create fear, Visa does not believe the limited risks warrant any inconvenience or additional expense to the cardholder.

Merchant double swiping

Double swiping refers to the act of a merchant completing a second swipe of a payment card at the point of sale after the card has been used to obtain authorization from the card issuer. In most cases, the second swipe is unrelated to authorization or settlement but is used to create a secondary record to support the merchant's accounting, reporting or customer-relationship management programs (e.g. loyalty and rewards).

Should there be a business requirement, acquirers and merchants can explore the integration of the Electronic Data Capture (EDC) with the Point of Sale (POS)/Cash Register system or otherwise have the merchant stop the practice altogether.

Elements of a Secure Payments System

Visa continues to work with the industry to roll out its five pillar security agenda to strengthen the payments system. This includes:

Visa card security features

The Visa card itself has a number of built-in security features designed to help card issuers and merchants recognise a real card from a counterfeit one. These include the chip, magnetic stripe, embossing, dove hologram and three-digit Cardholder Verification Value (CVV2).

Chip

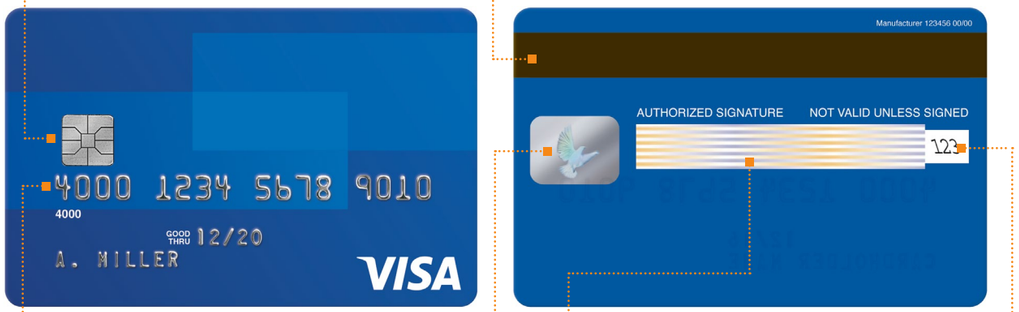
You may have noticed that more merchants are inserting your card into a chip terminal instead of swiping it when you make purchases.

That is a good thing because the microchip embedded in your card is virtually impossible to duplicate.

Powerful encryption prevents unauthorized access to information stored on the microchip, making electronic payments safer than ever before.

Magnetic Stripe

The magnetic stripe is encoded with the card's account number, expiration date, and other identifying information.



Account Number

The embossed or printed account number on your Visa card should begin with the number "4". The account number must be laid out in an even and straight manner.

On counterfeit cards, the numbers may have fuzzy edges or you may be able to see "ghost images" of the original numbers.

Dove Hologram

The Visa dove hologram should appear three-dimensional and appear to move when the card is tilted back and forth.

Many counterfeit cards contain a one-dimensional printed image on a foil sticker.

Signature Panel

The signature panel on the back of your Visa card has a tamper evident design. This is a personalization feature that matches you to your card.

If someone tries to erase the existing signature off the signature panel, you'll see the word "VOID" appear.

Card Verification Value

The Card Verification Value (CVV2) is a 3-digit code at the back of your Visa card.

When you shop online and retailers don't get to scan or swipe your card, this 3-digit code lets them know you have a valid Visa card in your possession.

If a fraudster obtains your account number, but doesn't know the security code, the purchase doesn't go through.

Chip technology

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. It is a proven solution as we have already seen a significant drop in counterfeit activities to negligible levels in several countries that have invested in chip technology.

Apart from being effective in preventing counterfeit activities, 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 has a global roadmap in place, to shift the financial impact to acquirers who continue to use non-chip acceptance devices.

Contactless technology

Visa's contactless payment technology Visa payWave is based on secure EMV chip technology. Visa payWave-enabled cards are as secure as any other Visa chip card and carry the same multiple layers of security.

See the Securing Future Payments section on page 17 for more on Visa's contactless payment security.

Verified by Visa

Verified by Visa is an online service designed to make internet transactions safer by authenticating the cardholder's identity at the time of purchase. Verified by Visa is one of several layers of security provided for online purchases.

Verified by Visa has been enhanced with banks migrating from the use of static passcodes to dynamic passcodes, such as "one time passcodes" (OTP), removing the need for cardholders to remember another password.

One time passcodes are sent to the cardholder's mobile phone or may also be generated via hardware tokens, making it easier to complete the authentication process, reducing transaction abandonment.

Visa's Account Information Security Program (AIS)

AIS is a global data security program that guides all stakeholders in the payment eco-system including merchants, third party agents, processors and banks, to secure payment card information in their network environments, to help protect against malicious attacks.

This program provides all stakeholders with an easy to use toolkit aimed to help them understand and implement data security related controls and processes.

The program provides global standards, a best practices guide, and a self-assessment questionnaire that helps the entity to evaluate its readiness to protect data. Visa has aligned its AIS program requirements to the global Payment Card Industry Data Security Standards (PCI DSS), the international standards for the payments industry. These standards are also adopted by all international schemes, therefore 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. 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.

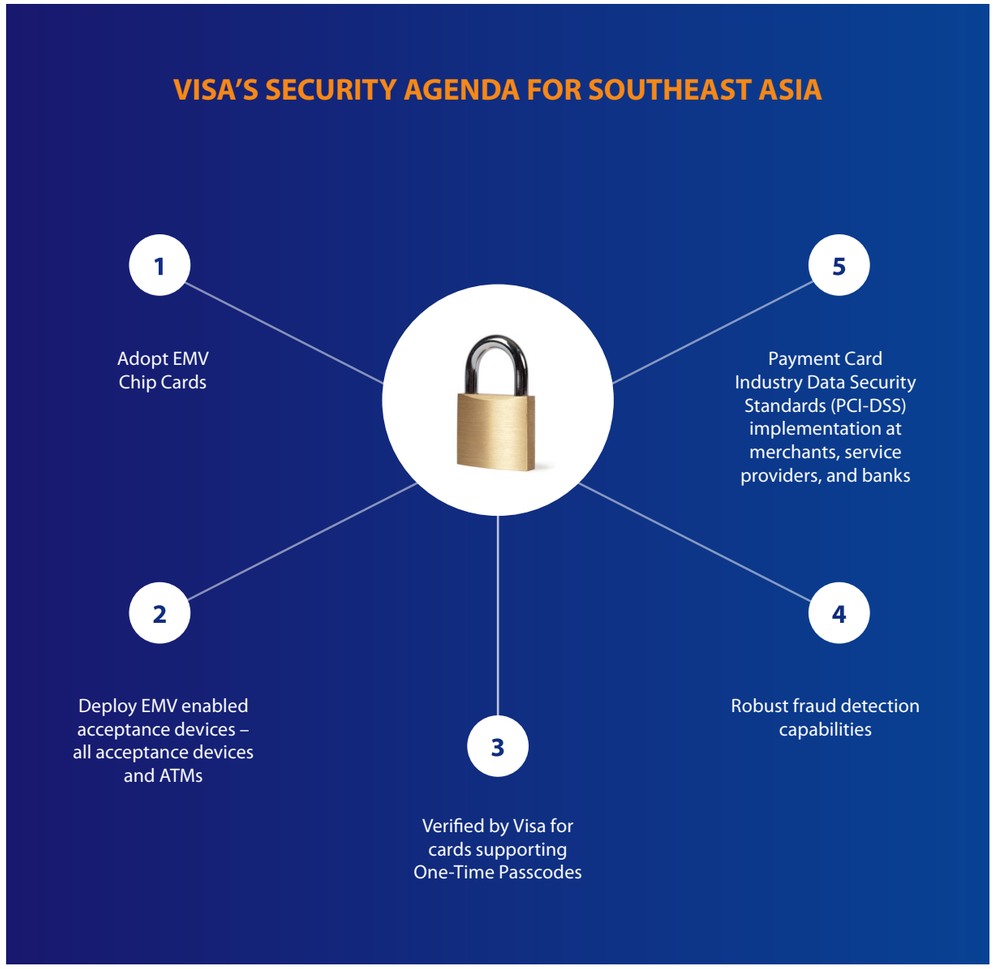
Industry cooperation

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 working groups aimed at enhancing industry wide security.

Visa's Security Agenda For Southeast Asia

Five Pillars

Security remains a top priority for Visa. In order to strengthen the payments system, we developed a strategy that is based on five pillars.



EMV 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), is a solution to counterfeit and lost and stolen card crimes. 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?

The roll-out of chip technology and other security measures has been effective in reducing unauthorized transactions in the physical card present environment. In addition, 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.

EMV Liability Shift

The EMV liability shift is applied to fraudulent transactions conducted with a counterfeit magnetic stripe from a chip card. As the migration to EMV chip has progressed throughout the world, the need for all regions to fully participate in EMV has continued to increase — in particular, issuers have expressed concerns about potential counterfeit risk exposure when their chip cards are used at US and AP-based magnetic-stripe-only ATMs.

In the past few years, Visa has announced liability shifts for both point-of-sale and ATM transactions in various countries. However, magnetic-stripe-only ATMs in the US and most AP countries remain the last significant area preventing issuers from maximizing the benefit of their EMV chip investment. Therefore, Visa is introducing liability shift dates for ATM transactions for the remaining regions:

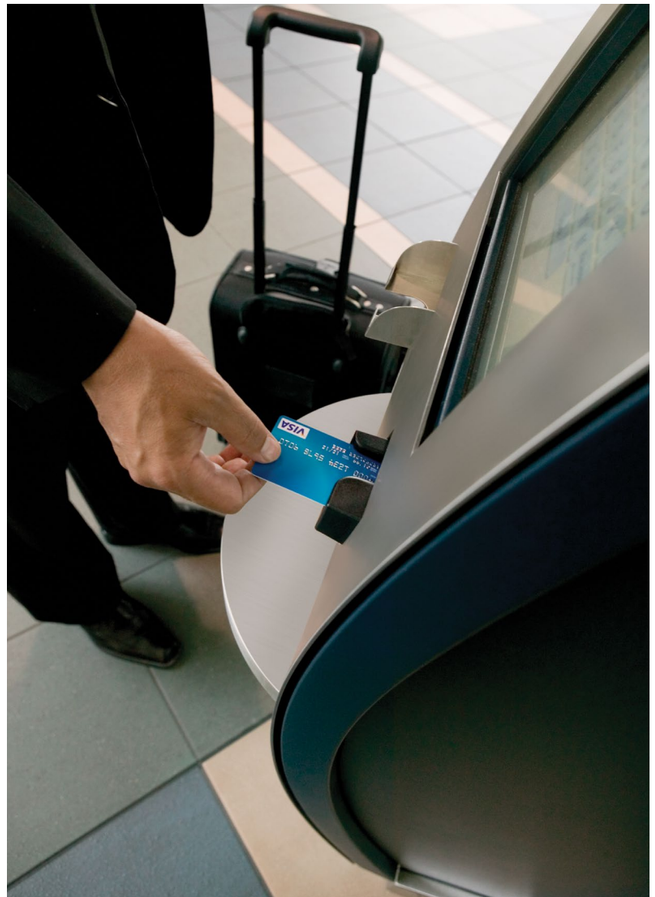
EMV ATM Liability Shift

Effective 1 October 2015
All countries excluding China, India, Japan, Thailand, USA

Effective 1 October 2017
China, India, Japan, Thailand, USA

EMV POS Liability Shift

Effective 1 October 2015
USA (excluding automated fuel dispensers – which is effective 1 October 2017)



Verified by Visa

Verified by Visa is an online service designed to make internet transactions safer by authenticating the cardholder's identity at the time of purchase. Verified by Visa is one of several layers of security provided for online purchases.

An essential layer of merchant security

With online security threats on the rise Verified by Visa provides an essential layer of merchant security.

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. 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.

One time passcode to mobile phones

Verified by Visa has been enhanced with banks migrating from the use of static to dynamic "one time" passcodes, removing the need for cardholders to remember another password.

One time passcodes are sent to the cardholder's mobile phone making it easier to complete the authentication process, reducing transaction abandonment.

Issuer Adaptive Authentication for eCommerce

Issuer Adaptive Authentication for eCommerce is an advanced implementation tailored to handle each and every Verified by Visa transaction according to its individual level of risk, challenging only those transactions deemed necessary.

Enhanced user interface

Visa has also enhanced and simplified the Verified by Visa user interface making it even easier for cardholders to use. Enhancements include the use of overlay web technologies to provide the following benefits:

- Allowing dynamic pre-messaging to prepare the consumer for the authentication process.
- Removing "pop-up" screens so the checkout page remains in the background to assure the consumer that they haven't lost their shopping cart.
- Reducing the possibility of lost sessions - consumers can easily navigate back to checkout.

Benefits of Verified by Visa for merchants include reduced security threats and chargebacks, reduced operating expenses, increased consumer confidence, easy implementation, marketing opportunities and lowered transaction fees.

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.

Robust Fraud Detection Capabilities

Identifying potential fraud attempts before they happen is often the best form of defense.

For Issuers

Ongoing monitoring of your transactions combined with risk intelligence will help you to detect new and emerging security threats, helping you to secure transactions at the point-of-sale, online or at the ATMs.

Visa Advanced Authorization and Visa Risk Manager are two solutions offered by Visa to help you to improve the accuracy of your risk detection. These tools provide you with greater visibility of your transactions and risk scoring capability which allows you to decline only the highest risk transactions.

All transactions that pass through Visa's processing network VisaNet are assessed by our Vital Signs service. This includes monitoring ATM transactions from around the globe 24x7 to detect potential ATM cash-out attacks. This free service informs the Issuer if one of their cards has triggered an alert and has been temporarily blocked. Issuers can request the block be removed if they regard the transactions legitimate. The Vital Signs service is designed to provide additional protection with minimal disruption to Issuers.

For Merchants and Acquirers

Information is the foundation of your fraud detection strategy. The more data you have, the more quickly and accurately you are able to detect fraud. It is imperative that both merchants and acquirers possess the capability to assess and process the vast amount of information about a transaction to stop fraud closer to its inception.

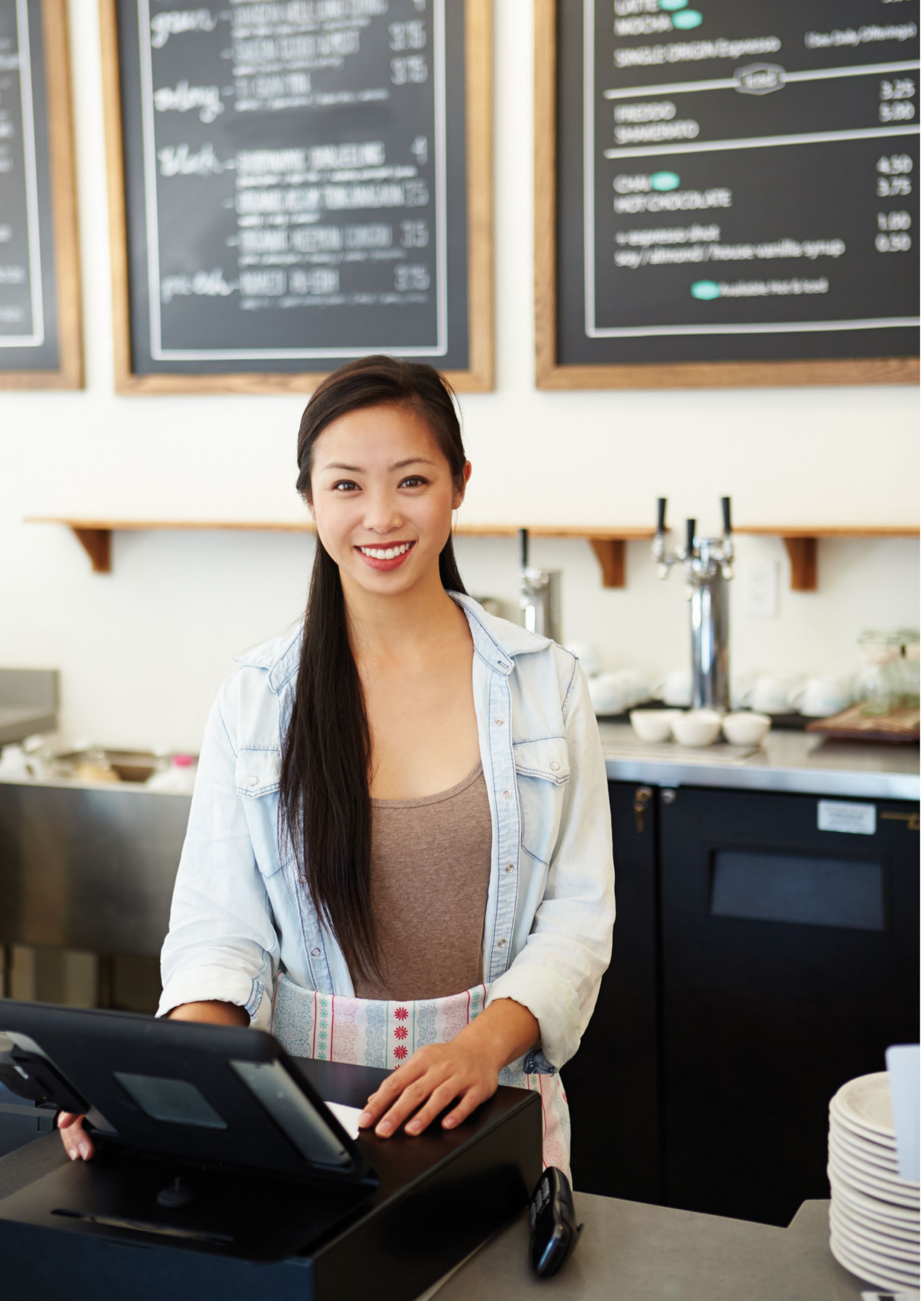
CyberSource is a global leader in fraud management, proven and deployed on six continents. The foundation is Decision Manager, a hosted fraud management portal with access to the world's largest fraud detection radar, a rules engine, a case management system, and reporting and analytics. With CyberSource, you can detect fraud sooner and more accurately, streamline fraud management operations, and scale easily as your business grows.

Data Breach Detection

Events are monitored locally, regionally and globally. Trends are identified and risks continually assessed.

In the event of a data breach Visa will:

- Work with the compromised entity to contain the breach
- Identify card numbers deemed at risk and distributes them to Issuers via CAMS
- Collaborate with Law Enforcement on payment card investigations
- Require PCI DSS compliance for the breached entity as part of the remediation strategy



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, or on the phone 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.

Merchants who do not need to process card data can simplify their PCI-DSS compliance by eliminating "double swiping" or completing a second swipe of a payment card at the point of sale after the card has been used to obtain authorization from the card issuer. Please see Payment Security Concerns on page 05 for more information.

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 www.visa-asia.com/secured.

Securing Future Payments

At Visa we've been working hard to provide our cardholders with more convenient, efficient, simple and secure payment options. With every new product or innovation we create security remains one of our highest priorities.

Contactless payments

Contactless payments are growing in popularity as cardholders realize they meet the fundamental need for speed in places such as convenience stores, sporting venues and fast food restaurants. Across Southeast Asia, we have developed contactless payment systems that make transactions faster, safer and more convenient than cash, particularly for small value transactions.

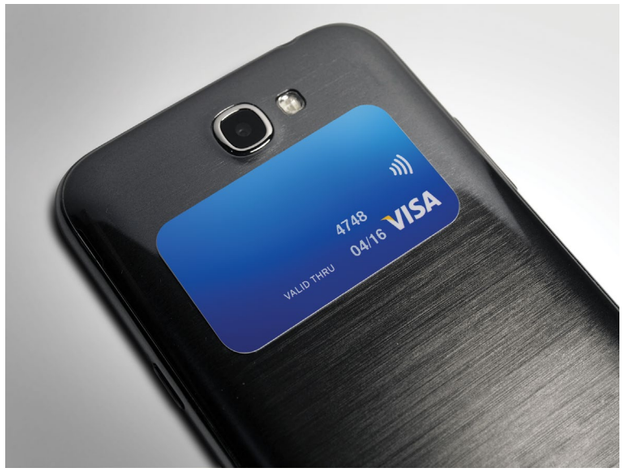
Visa payWave

This is Visa's contactless payment technology based on EMV chip. Cardholders just wave and go – there is no need to sign or PIN for purchases under the predetermined transaction limit and no need to swipe or dip either. You just hold the card against the contactless reader and it allows a fast transaction in less than one second.

Visa payWave-enabled cards are as secure as any other Visa chip card and carry the same multiple layers of security. In addition, with Visa payWave, the card never leaves your hand, which reduces the risk of fraud.

Contactless card technology uses applications that protect personal information and are designed to deliver fast, secure transactions. The security features of Visa payWave cards include:

- Ultra short read range
- Based on the secure global EMV chip platform
- Usage of encryption keys and strong cryptographic techniques on every transaction
- Restricted write capabilities – only the authorized issuer is able to write or change payment related data
- A secure microprocessor
- The systemic risk management procedures and fraud detection capabilities of the Visa processing system.



Payment Tokenization

Payment tokenization is the process of replacing the traditional 16-digit payment card account number with a unique digital account number or "token" for use in online and mobile transactions. Tokens can be restricted to transactions with a specific mobile device, merchant, or transaction type.

Tokens help to simplify the purchasing experience for consumers by eliminating the need to enter and re-enter the account number when shopping on a mobile phone, tablet, or PC. Tokens or digital account numbers also help to prevent fraud in eCommerce and mCommerce transactions by removing sensitive card account information from the payment process.

Apple and Visa issuers in the U.S. are the first to take advantage of the new Visa Token service, allowing Visa account holders with the new iPhone 6 and other Apple devices to make secure in-store, in-app payments and mobile NFC transactions.

Mobile point-of-sale

In the last five years mobile technology has created new ways of thinking about point-of-sale that can save customers from waiting in long queues, reinventing the traditional store check-out process.

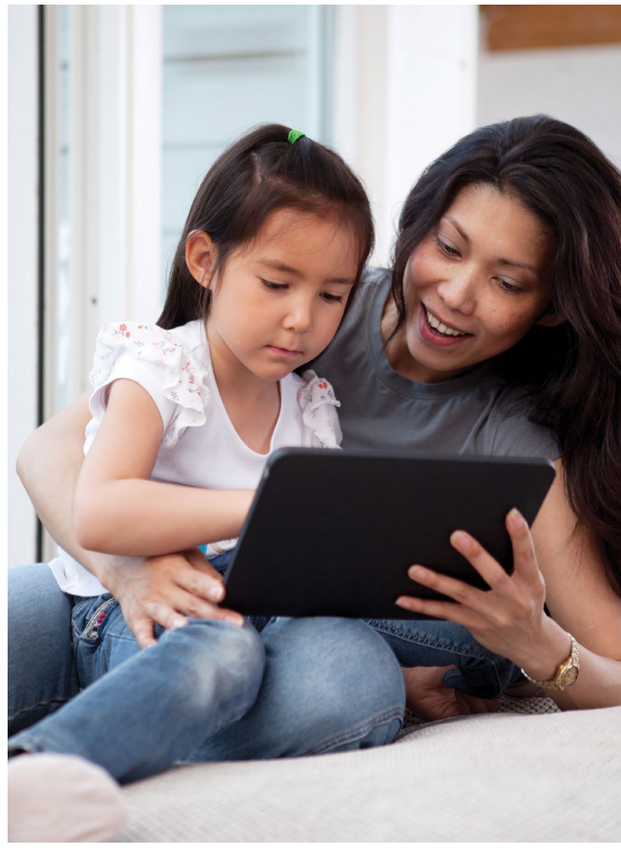
New payment innovations known as mobile point-of-sale (mPOS) devices can convert a mobile phone or tablet into a secure card payment processing terminal. Now merchants are taking advantage of transacting from anywhere, effectively bringing the POS to the customer.

When considering mPOS the following security measures should be adhered to:

- Ensure POS terminals are chip-compliant for increased security
  To prevent unintended consequences from the misuse of a mobile payment acceptance solution, ensure that the solution is used in a manner consistent with the guidance provided by an acquiring bank and solution provider.
- Limit access to the mobile payment solution to avoid exposure of account data that may be used to commit fraud
  Merchants are encouraged to use a passcode, password or security pattern to lock their mobile device when not in use. Configure the device to auto-lock after a number of minutes of inactivity.
- Immediately report the loss or theft of a mobile device or hardware accessory
  Contact the acquiring bank immediately to report the loss or theft of a device or accessory in order to take the necessary actions.
- Install and regularly update the latest anti-malware software
  Merchants should regularly update the firmware of their device and install any application updates whenever a new update becomes available. Don't 'jailbreak' or 'root' the mobile device; this will increase the risk of malware infection.
- Install software only from trusted sources
  It is strongly recommended to abide by any security measures recommended by the mobile device and install only trusted software that is necessary to support business operations and to facilitate payment.

Looking to the future

As we look to the future, payment products will continue to evolve. The convergence of the Internet and mobile technologies are creating new demands for electronic payments. Today, consumers want the ability to easily pay online, via mobile phone or in social networking/gaming environments. Similarly, merchants are looking to payments companies to provide the innovation and leadership needed to keep pace with these rapid developments.

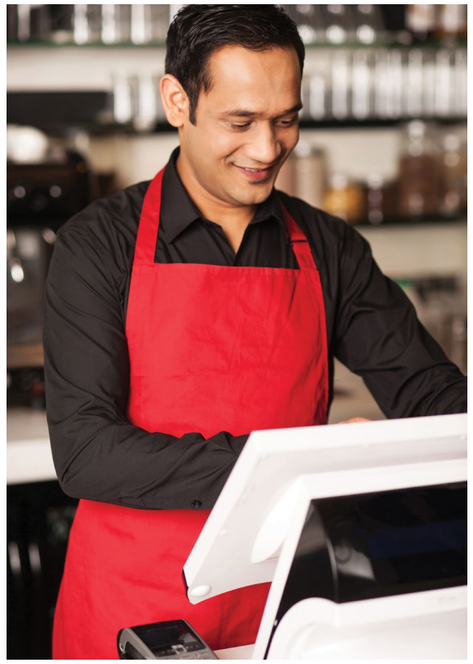


Merchant Safety Tips

Here are some security steps merchants should follow when accepting electronic payments:

Card Present Merchants

- Complete the transaction as required by your bank, which at a minimum includes obtaining authorization and getting the cardholder's signature on the transaction receipt.
- Politely ask for an identification document for verification if you feel the purchase amount is unusually large or if cardholder behavior is suspicious.
- Inspect the card security features to make sure the card is valid and has not been altered.
- Use EMV chip readers to enable chip transactions. Chip processing strongly mitigates counterfeit fraud.
- Hold the card and call your bank if you feel suspicious of the card or cardholder.
- For cancelled transactions, always process a refund back to the card with a Visa credit receipt. Never refund in cash for returned merchandise.
- If you are handling an unsigned card, first check the cardholder's ID. Ask the customer to sign the card and compare the signature on the card to the signature on the ID.



Card Not Present Merchants

- Participate in fraud prevention solutions such as Verified by Visa (VbV) and Card Verification Value 2 (CVV2).
- Use Fraud Monitoring tools to mitigate fraud (some transactions may not be fully authenticated as Cards or the Issuing banks are yet to deploy VbV solution).
- Encrypt data sent across networks, e.g. Use strong cryptography to secure communication between the cardholder and your internet systems (SSL 128 bit).
- If possible, take note of a contact phone number (preferably not a cell phone number) and the name of the financial institution that issued the card.
- If you are taking an order over the telephone, record the time and date of your conversation and make a note of the details of the conversation.
- If you are taking an order through the mail or via a fax, obtain a signature on the order form, always retain a copy of the written order, and get proof of delivery.
- Include content or features on your website to promote ease of use for online shoppers and reduce cardholder disputes and potential chargebacks (e.g. Complete description of goods and services; customer service contact information including email address or phone number; return, refund and cancellation policy; delivery policy; country of origin).

Data Security

- Secure your POS devices and always keep them within sight of authorized users.
- Ensure you comply with PADSS & PCIDSS requirements.
- Do not double swipe on unsecured / non PA-DSS certified POS systems as it exposes magnetic stripe full track data to compromise. If card information is required, integrate your magnetic / chip card reader with POS system and transmit only non-sensitive information.
- Install and maintain a firewall configuration to protect data.
- Use and regularly update anti-virus software.
- Do not use vendor-supplied defaults for system passwords and other security parameters.

Cardholder Safety Tips

Here are some basic steps to help cardholders to 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 and sales receipts.
- If your card becomes 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 receipts including the purchase amount when you sign them.
- 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 payment 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:

Register for Verified By Visa

Verified by Visa is a free, online service designed to make internet transactions safer by authenticating the cardholder's identity at the time of purchase.

Use a secure web browser

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

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.