



UNDERSTANDING A DATA COMPROMISE AND HOW TO RESPOND

A Communications Guide for Issuers



Who Should Use this Guide:

Front-Line Marketing, Communications and Product Contacts at Issuing Financial Institutions.

Purpose:

Protect cardholder trust in payments by providing a practical guide to managing communications after a data compromise at a third party.

Table of Contents

Surveying the Landscape: Situation Analysis	2
Leading the Way: Crafting a Solution	3
Payment Card Fraud Primer: An Overview of Data Security Threats	4-7
Visa’s Risk Response: A Brief Guide to Visa’s Risk Procedures and Policies for Handling a Data-Compromise Event	8-9
Communicating in a Crisis: Dealing with the Communications Challenge of a Security Breach	10-13
Communications Tactics: Sample Materials	14-15
Glossary of Terms.....	16-17



Surveying the Landscape: Situation Analysis

“Data breach.” Just a few years ago, only a handful of people in America had heard the term. Today for tens of millions of Americans, it is synonymous with a virulent new threat to their financial well-being. Hacking, identity theft, dumpster diving – all these terms have gone from the fringes of society to becoming deeply embedded in our everyday lexicon.

As financial services industry professionals, the challenge of managing this increasingly complex environment is an ever more urgent priority. The risk posed by data theft is not just about the money that can be stolen, but also about the unique way in which it undermines confidence and trust in the entire payment system. And when consumer confidence is allowed to erode, then the foundation of the entire economy may be jeopardized.

That is why it is critical to develop a clear understanding of consumers’ changing perceptions and expectations when it comes to the security of their valuable private information. This is especially true for the individuals or teams charged with the responsibility of managing customer relationships and corporate reputation.

“We are in a crisis of trust.”

CMO Council, Secure the Trust of Your Brand Report



In the fight for payment card security, it isn't enough to make our systems as heavily protected as possible. We must also work together to ensure that we are equally vigilant in safeguarding the public's trust in their financial institutions and payment networks. Consumers must know that every measure is being taken to keep their data secure, and that when breaches do occur, that they are handled quickly and responsibly, with consumers' best interest always kept top-of-mind.

With that guiding principle in mind, this manual is designed to **provide useful tools for front-line marketing communications and product managers at financial institutions to better protect cardholder trust through effective breach-response communications**. The materials provided here, combined with your own communications infrastructure, are intended to help your organization communicate how the situation is being managed and that customer concerns are being addressed in a clear and confident voice.

In this manual, you'll find the following information and tools:

- **Payment Card Fraud Primer:** An overview of the nature of data security threats.
- **Visa's Risk Response:** A brief guide to Visa's Risk procedures and policies for handling a data-breach situation and how the group coordinates with your Risk team. This background information is important to understand because much of the content and timeline stem from the facts associated with the event.
- **Communicating in a Crisis:** An overview of how Visa recommends dealing with media and customer communications surrounding a data compromise.
- **Communications Tactics:** A communications toolkit, including sample customer letters and insert, customer service Q&A, and a reactive press statement.

It is important to note at the outset that the suggestions contained in this manual are meant to serve only as a general resource. Every data-compromise situation is unique. Your organization's response should be tailored to meet the specific circumstance. However, by reviewing the general principles and tools contained in this manual, we hope that you can begin to prepare your organization so that should an event occur, you will be well-positioned to act decisively. In the end, that is what can make the difference between a data-breach incident that is contained and managed, and one that could threaten your organization's core relationship with your customers.

Payment Card Fraud Primer: An Overview of Data Security Threats



Before getting into the details of how to best respond to a data breach, it is critical to understand both the nature of the threat and the measures that are in place to meet those threats. Any communication from your organization during a possible data-breach situation should be based on a firm understanding of the issues involved and the measures that are in place to protect consumers.

In their efforts to commit fraud, criminals are on the lookout for points of weakness. They understand that in every network, data must pass between multiple hands. Their goal is to find that one unprotected link in the chain.

FRAUD TYPE	TOTAL 2004	TOTAL 2005	TOTAL 2006
LOST	\$152,421,080	\$202,099,981	\$165,497,172
STOLEN	\$254,945,941	\$257,133,673	\$246,145,918
NOT RECEIVED AS ISSUED (NRI)	\$24,037,125	\$30,574,829	\$35,475,553
FRAUDULENT APPLICATION	\$35,937,003	\$42,379,746	\$54,875,579
COUNTERFEIT	\$219,232,191	\$379,679,515	\$471,625,042
MISCELLANEOUS	\$35,867,693	\$60,413,635	\$61,296,819
ACCOUNT USE	\$351,398,267	\$404,612,391	\$510,093,477
FRAUD RATE	0.2006%	0.2374%	0.2349%

Within the Visa system, fraud has remained at low levels, but more must be done to keep it there.

Today, counterfeit fraud is the fastest growing fraud type, with a year-over-year increase of 75 percent, and second to card-not-present fraud. Counterfeit fraud involves criminals stealing a customer's card information through skimming or a data compromise and creating a fake card. Customers, not having lost the physical card, will spot fraudulent transactions on their account. Other fraud types include lost and stolen cards, identity theft and not received as issued.



Setting the Standard in Security

Protecting cardholder data is the best front-line defense to prevent fraud, especially counterfeit and card-not-present types. In fact, it's the single best defense for a merchant or processor to reduce its risk of being a victim of a data compromise. Since 2001, Visa has required that all merchants and service providers that store, process, or transmit Visa cardholder data adhere to the highest security standards. Today, no merchant or processor that has been compliant with the industry's data security requirements, known as the Payment Card Industry Data Security Standard (PCI DSS), has ever experienced a data compromise.

PCI DSS

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. For more information, go to www.pcisecuritystandards.org

Fraud Type Definitions

Lost: The card was lost or misplaced.

Stolen: The card was stolen.

Card Not Received as Issued (NRI):

The cardholder did not receive the issued card; although, the issuer confirms that it was sent to the cardholder.

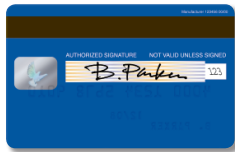
Counterfeit: The cardholder did not knowingly participate in a transaction, or the issuer confirms that such an account was never issued, but the card's magnetic stripe was used in a card-present environment and unlawfully altered or duplicated.

Card-Not-Present: Any fraudulent transaction where the card was not physically presented to the merchant such as an Internet purchase or a mail-order/telephone-order purchase.

Identity Theft: Includes a fraudulent application and account takeover where another party has unlawfully represented itself as the cardholder.

**Payment Application
Best Practices (PABP)**

- Don't store full magnetic stripe data or CVV2
- Protect stored data
- Provide secure password features
- Log application activity
- Develop secure applications
- Protect wireless transmissions
- Test applications to address vulnerabilities
- Facilitate secure network implementation
- Cardholder data must never be stored on a server connected to the Internet



Magnetic Stripe

Important, sensitive information is stored on the card's magnetic stripe. Storage of this data is prohibited and can increase a merchant's or processor's risk of becoming a data-compromise victim.

Criminals Target Card Data

Card data has become as valuable to thieves as merchandise or cash. Data from a single transaction can touch up to as many as 50 different entities – from financial institutions to processors to merchants – on its path from swipe to settlement.

This rich card data is what criminals need to create fake cards and use them fraudulently. Specifically, they are looking for what we call “track data.” It's the secret information embedded in the magnetic stripe of a credit and debit card. This stripe contains the cardholder's 16-digit account number, the expiration date, the cardholder's name, and something known as the Card Verification Value (CVV), a three-digit code that is required to deter counterfeiting. Another secret code on the card is the Card Verification Value 2 (CVV2), located next to the signature panel on the back of the card. When all this information is stored by a merchant and then compromised, the criminal has all he needs to replicate a customer's card and use it fraudulently.

And if the merchant is storing the prohibited PIN data in addition to the magnetic stripe data, then the crime can migrate from the point of sale to the ATM. Nearly 100 percent of data compromises between July 2005 and October 2006 involved full-track data.

What you might not know, is that these criminals are seeking this data from a myriad of sources including brick-and-mortar merchants, e-commerce businesses, and financial institution processors and agents. In analyzing the data compromises reported to Visa since July 2005, they are evenly split between brick-and-mortar and e-commerce merchants. Even the type of merchant varies, with restaurants suffering the largest number of compromises, followed by universities and clothing retailers.

The strongest commonality among the merchants was the storage of track data caused by their point-of-sale software systems. Often, even without the merchants' knowledge, their card acceptance systems were storing this valuable data, increasing their risk of being hacked.

That's one reason Visa created the Payment Application Best Practices (PABP) in 2005 and is actively advocating it to become part of the industry's PCI DSS requirements. The best practices are designed to assist software developers create secure payment applications that prevent data compromises and ensure that prohibited card data isn't stored.

Visa Targets Greater Security

The good news is that while data thieves are working to find weaknesses to exploit, Visa, merchants, and member financial institutions are working even harder to keep customer data secure. Visa alone is investing more than \$200 million a year to secure electronic payments.

This investment is at the heart of Visa's security strategy based on multiple layers of security. These layers include:

- **Securing the payment environment** to protect card data and render it useless to thieves by:
 - Utilizing industry standards, like PCI DSS, to reduce weak links.
 - Developing best practices to ensure that data is not improperly stored.
 - Creating next-generation authentication techniques to make sure that compromised data cannot be used by criminals to commit fraud.
- **Monitoring, identifying, and preventing fraud** through technology and best practices:
 - Deploying cutting-edge technologies to spot fraud and stop it, including **Visa Advanced Authorization**.
 - Creating personalized **Real-Time Decisioning** to enable issuers to automatically decline risky transactions.
 - Reinforcing current data storage prohibition rule and integrating the **Plus ATM Network** into VisaNet.
 - Enhancing fraud reporting to populate detection services, such as Advanced Authorization, with more data.

Taken together, these multiple layers, in addition to the investments made by your financial institutions, help ensure that when criminals try to obtain and fraudulently use cardholder data, they find themselves running into one wall after another.

However, even with the success of these efforts, data breaches sometimes do occur. In the next section, we lay out the precise steps that Visa takes when a data breach occurs.

VISA ADVANCED AUTHORIZATION

Only Visa provides real-time risk management technology that continuously monitors the VisaNet system for unusual, high-risk activity – including Verified by Visa profiles and compromised behavior patterns. When high-risk activity is detected, event-level risk information is sent to issuers in the authorization message, enabling early identification of fraud. As new forms of fraud evolve or new information is available, Visa Advanced Authorization adapts. Advanced Authorization also assesses the

probability of fraud at an account level. Issuers that presently use Visa Advanced Authorization have reported very low false positives and bottom-line reductions in gross fraud loss of up to 30 percent.

Issuers should check with their processor for availability. Alternatively, Visa provides access to the information through a workstation at Visa Online for a minimal fee.

Visa's Risk Response: A Brief Guide to Visa's Risk Procedures and Policies for Handling a Data-Compromise Event



Any discussion of data compromises must begin with a clear definition of what actually constitutes a breach. For Visa's purposes, a security breach can be defined as an event in which cardholders' personal information is exposed to a high risk of theft. Importantly, not every security breach leads to fraudulent activity. However, the moment that cardholder data has been exposed, Visa's policy is to proceed with an abundance of caution in order to mitigate the risk of fraud occurring and to limit the extent of fraudulent activity, should it occur.

Below, we outline the steps that Visa goes through when a data breach occurs.

Step One: Spotting a Potential Breach

There are a number of ways in which Visa can learn of a potential data breach. Oftentimes, a financial institution will identify a fraud pattern and will determine a common point of purchase or merchant that could be the source. Similarly, there are occasions when acquirer banks will spot potential fraud activity emanating from one of their merchant customers.

Visa also monitors its own system 24/7/365 by using sophisticated neural networks to identify potentially fraudulent activity. This technology allows us to execute real-time analysis to identify a potential breach point.

In either of these circumstances – whether the potential fraud activity is spotted by a member financial institution or by Visa – the response sequence is immediately triggered.

Step Two: Determining Whether a Breach has Occurred

Once a possible breach has been spotted, Visa commences an investigation whose first aim is to determine whether, in fact, a breach has occurred. As noted above, not every act of fraud is the result of a data breach and not every data breach leads to fraud. Our initial investigation seeks to swiftly determine the nature of the incident in question.

The investigation process unfolds in the following few key steps:

- A case file is opened, and a Visa team is dedicated to the task.
- The acquirer bank is informed of the investigation.
- Visa begins to gather pertinent details and facts such as:
 - Whether the possible breach was based on card-present or card-not-present transactions.
 - The kind of software that was used in the merchant's payment application.
 - The data that was being stored – in particular, whether full-track data was being stored in contravention of Visa operating regulations.

In order to confirm that a breach has taken place, Visa looks for a threshold of indexes:

- Multiple reports from issuers – normally at least four separate institutions.
- Other card schemes indicating a potential breach for their cardholders at the same point-of-sale.
- A spike in the level of fraud being reported from a single source.

- The use of payment application software with known weaknesses at the point-of-sale or other PCI-compliance failure.
- Issuers reporting more than 999 accounts identified as having fraud tied back to that location.

Step Three: Investigation and Mitigation

Once a breach has been confirmed, Visa then moves into a rapid response on two parallel tracks: investigating the incident and making sure that potentially compromised data is not used to commit fraud.

On the investigation front, we operate according to the following process:

- First, we seek to open a channel for information-sharing between the acquiring bank, other card systems, as well as the compromised merchants and potentially impacted issuers.
- If the issuers have already contacted law enforcement, we work with the relevant agencies (typically the United States Secret Service) to offer our assistance in their efforts.
- Then we contract with an independent forensic company to come in and execute a swift examination of the circumstances surrounding the breach, with a particular emphasis on determining as quickly as possible:
 - How the breach occurred.
 - How much data was compromised, and what the nature of the data was.
 - What the possible sources of the breach may have been.

At the same time as we are conducting this investigation, we are working to feed information gleaned from the investigation into our security system to mitigate the impact of the exposed data.

Toward that end, Visa takes the following steps:

- First, we ensure that the breach is sealed. This includes having the potentially affected merchant remove track data and/or shore up its wireless system in order to ensure that no more accounts are put at risk.
- Once we have secured the breach, we then quickly analyze the potentially exposed accounts and put out a Compromised Account Management System (CAMS) alert that identifies at-risk accounts. This CAMS alert is often your financial institution's first notification from Visa about an event and is sent to your Risk department. This alert contains details about the situation and provides impacted account numbers for monitoring or reissuance by your institution. We encourage you to ask your Risk executive to notify you when a CAMS alert is received. This will often start your communications preparedness process.
- Account information is simultaneously uploaded into our industry-leading Advanced Authorization system to ensure that if data thieves try to make purchases using the compromised account data, we will be able to spot the activity before the transaction is completed and the issuer will have the opportunity to decline the transaction.
- Finally, we hand off the mitigation work to the PCI team to make sure that the merchant becomes fully compliant with PCI DSS so that no future compromises will occur from the same operation.

Communicating in a Crisis: Dealing with the Communications Challenge of a Security Breach



Audiences to Consider When Planning Communications

- Cardholders
- Regulators
- Legislators
- Merchant customers
- Employees
- Agents/processors
- Customer service
- Shareholders
- Analysts
- Media
- NGOs
- Partners

As noted in the introduction, every data compromise is unique. In a crisis, your communications team will be dealing with a series of tough questions that need to be analyzed and answered quickly: What are our requirements to notify regulators? Are there applicable state disclosure laws that require us, as an acquirer or issuer, to disclose to our customers? Will business actions, like reissuance of a card or PINs, create potential customer concern? Is the compromised entity planning to disclose that it was breached, causing an increase in reissuance requests and other customer service issues?

These are but a few questions to address, some of which can be answered in advance of a security crisis. But taking the time to prepare for these circumstances is a critical investment that offers a real return.

According to a study from the Chief Marketing Officer (CMO) Council, more than half of U.S. consumers would either strongly consider or definitely take their business elsewhere if their personal information was compromised. Additionally, Emory University researchers found that a company loses, on average, from 0.63 percent to 2.10 percent value in stock price when a breach is reported. This is equivalent to a loss in market capitalization of \$860 million to \$1.65 billion per incident.

Assuming a Leadership Position

When it comes to your company's reputation, few consumers can actually cite a specific brand that they associate with having a trusted reputation for protecting its customers' security. Likewise, respondents also had trouble naming a brand associated with having a tarnished reputation for protecting customers' security. This lack of customer trust mind share, good or bad, represents a significant opportunity for marketers and communicators to use as a competitive differentiator.

Consider the following suggested operating principles for successfully managing communications around a security incident:

- **Focus on the Facts.** Successful navigation of any security-breach situation begins with having a clear grasp of the precise facts of the case. The media, customers, and other stakeholders will be searching for information. Being able to serve as an authoritative source reduces the risk of harmful rumors and provides greater control.
- **Understand Roles and Responsibilities.** Managing the communications around a security breach demands a disciplined response. Reducing incidences of multiple voices – either between organizations or within a single organization – will reduce confusion and build confidence. Toward that end, it is important to establish clear lines of communication with Visa to share information and updates. And within your organization, it will be helpful to have in place a clear and rapid response plan that designates roles to each player and a dedicated decision-making team ready to gather quickly when the need arises.
- **Weigh the Costs and Benefits Carefully (And Remember What's at Stake).** Deciding what information to communicate to customers, the media, and other stakeholders is one of the greatest challenges that financial institutions face in the midst of a security breach. What is critical is to have in place a process for making these decisions on the basis of a clear sense of what each decision could cost and what benefits it could deliver. In these calculations, it is important to remember that part of the calculus should be the long-term trust and confidence of your customers and cardholders everywhere. Every decision should be made in light of these critical stakes.

Crafting an Effective Communications Response

Cardholders are realistic. They accept that security breaches will happen. What they expect is that no effort will be spared trying to prevent breaches and that if a breach does occur, the response will be swift and that their interests will come first. To assist issuers in creating breach-response messages, Visa conducted a series of cardholder focus groups in November 2006 to better understand what cardholders want and expect in the event of a breach.

In the following sections, you will find research-based recommendations for handling card reissues and breach-notification best practices. Although every issuer knows his/her customers best and must tailor a response to meet their specific needs, Visa provides template materials, including sample cardholder notification letters, call center scripts, and a reactive press statement.

What Cardholders Want/Expect

When a data compromise happens, cardholders want their financial institutions to go the extra mile to minimize inconvenience, protect them from any cost of fraud and provide timely, relevant information about what happened. They want and need your assurances that the event will have little to no impact on them.

A few specifics for consideration: Cardholders place a high value on immediate notification if their accounts are part of a compromise – preferably within 24 hours. Cardholders also want details and communications through multiple channels, especially if they may experience an interruption in the use of the card.

Operationally, if cards are to be reissued, consumers want to receive their new plastic within seven days of notification (though 48 hours was the preference), along with more detailed information about the breach and what actions they should take to protect their account.

A one-page letter sent with the reissued card, if applicable, is the most effective and expected way to deliver this information to a wide audience. Consumers also consider a live phone call, automated call, or e-mail as appropriate secondary communication tactics. Especially if a card is being reissued, cardholders emphasize their desire to be contacted a minimum of two times.

What to Say

Cardholders underscored the importance of including critical pieces of the puzzle, with the main objective of understanding and being on alert for fraudulent activity. A data compromise can make cardholders feel vulnerable and threatened; providing detailed communications can help alleviate their concerns.

For any notification or reissuing communication, **first address the specifics of what happened and what to expect in terms of your institution's response.**

- The initial notification should describe the situation. Cardholders generally want details on the breach, including the merchant name. If such information cannot be shared, it is important to indicate why not (for example, because of an ongoing investigation).
- In Visa research, consumers reacted negatively to language they construed as vague and/or alarming. This included statements like “security breach,” “data compromise,” and “exposed.”
- Broad terms, like “card information” rather than “card number,” suggested that the impact was broader and invoked fears of identity theft. “Card number” was more contained and, therefore, more acceptable to consumers.
- Do not use the communication as an opportunity to promote other goods/services; it will dilute the primary objective and turn off cardholders.
- **If card is reissued**, let customers know when to expect the new card, when they should stop using their current card, and if there will be any change in PIN. It should include a 24/7 phone number for customers to contact, as well as direct them to the financial institution's Web site for further information. If possible, give cardholders the option of picking their new card up at a branch office – an option they want so that use of their cards can be restored faster.

After providing details about what happened, **second reassure cardholders of the layered security protections within your organization and Visa.**

- Reassure cardholders that they are protected from unauthorized transactions by Visa's Zero Liability policy and/or individual financial institution security product(s).
- Include information on what is being done to assure cardholders that fraud either won't happen or won't happen again.
- Acknowledge that the problem will be an inconvenience.

Visa research also reinforces the interest of cardholders to be empowered as part of the solution. Because cardholders will willingly take steps to protect their information and prevent fraud, **third encourage their engagement.**

- Instruct cardholders to monitor their accounts for unusual activity.
- Encourage cardholders to check their credit reports. Include credit-reporting agency toll-free numbers and Web site addresses for free credit reports. Remind them that they can get a free credit report each year.
- Reinforce that cardholders should immediately contact their card issuer if they notice unauthorized activity.

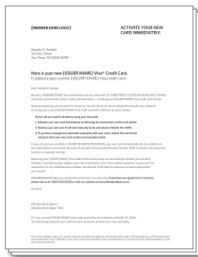
And last, but not least, expect that cardholders will have questions. **Include contact information, and prepare your customer service front lines.**

- Include toll-free contact numbers for cardholder questions. Ideally, this line is available 24 hours a day, 7 days a week.
- Don't forget to include a Web address.

Communications Tactics: Sample Materials



In this toolkit, we've prepared several sample materials that can be tailored to meet your customers' unique needs. Electronic files (in a variety of formats) for all of the documents may be found on the enclosed CD.



First, you will find three sample cardholder breach-notification letters ranging from general notification to specifically reissuing a credit or debit card.



Second, we have included a sample Customer Service Q&A to effectively manage cardholder concerns.



Third in the package is a sample cardholder statement insert that reinforces cardholders' protections and steps that they can take to protect themselves from fraud.



And last, we have included a Reactive Press Statement, should your organization receive a reporter call about a third-party compromise.

All of these materials are also available at Visa Online (www.visaonline.com).

Measuring Success

Ultimately, it will be critical to measure the success of your communications efforts. Since security challenges are a fact of life, it is important to learn from each incident so that mistakes can be avoided and practices improved.

In developing a protocol of measuring success, the following metrics could be considered:

- **Consumer Attitudes.** How secure do cardholders feel about using their cards? How secure do they feel about their cards relative to cash? Checks? To a competitor's card brand? How do they rate your organization's performance in handling the situation? How confident are they in your organization today relative to how they felt before the breach?
- **Usage.** Have impacted cardholders reduced or stopped using their check or credit card? Have there been noticeable behavior changes compared with historical norms? Are there significant usage differences between impacted and non-impacted customers? Between Internet and brick-and-mortar transactions?
- **Activation Rate.** Are there changes in activation rates? Are these changes comparable with historical norms? Are there significant differences in activation rates for consumers who have received a replacement card more than once in the past year?
- **Media Output.** How many stories appeared in the media that mentioned your organization by name? How frequently did your key messages come through in the coverage (e.g., the fact that consumers are protected by Zero Liability)?

Conclusion

Maintaining trust in the payment system is one of the greatest business imperatives financial institutions face today. Consumers who feel insecure about their data will use their cards less frequently. That harms every stakeholder in our system.

We can all do our part to combat this threat by making sure that when a security breach does occur, we respond to the situation in a manner that meets consumers' needs and expectations. And as noted repeatedly throughout this toolkit, the best approach to cardholder communications can be summed up in a single word: *straightforward*.

Cardholders want to know the steps they can take to prevent fraud, protect their data and how they should act in the event that a breach exposes their data.

By using strong, proactive communications, utilizing the full spectrum of available channels, you can help prevent the fraudsters from stealing the one thing that matters the most: customer trust.

Glossary of Terms

ACCOUNT TESTING

A fraud scam used by criminals to verify whether an account number is currently valid. To “test” an account, the perpetrators make a small purchase on it or they will submit an authorization request but not a sales transaction receipt. If the account is valid, it may then be used for additional, larger fraudulent transactions.

ADDRESS VERIFICATION SERVICE (AVS)

AVS allows merchants that accept card-not-present transactions to compare the billing address given by the customer with the billing address on the card issuer’s master file before shipping an order. AVS helps merchants minimize the risk of accepting fraudulent transactions in a card-not-present environment by indicating the result of the address comparison.

ADVANCE AUTHORIZATION

Advanced Authorization is a comprehensive Visa risk management tool that monitors and evaluates 100 percent of U.S.-issued VisaNet authorizations in real time. It is the first system of its kind to assess transaction data on an account-level and event-level perspective and deliver risk indicators in real time as part of the authorization message. Visa issuers are provided with risk information necessary to identify emerging fraud schemes and stop fraud before it starts.

AUTHENTICATION

The process of verifying the true origin or nature of the sender and/or the integrity of the text of a message or card.

CARD-NOT-PRESENT

A merchant, market or sales environment where transactions occur without a valid Visa card being present. Card-not-present is used to refer to mail-order/telephone-order merchants and sales environments as well as the Internet.

CARD-PRESENT

A merchant, market or sales environment where a transaction can be completed only if both a valid Visa card and the cardholder are present and the sale is processed by an individual representing the merchant or acquirer. Card-present transactions include face-to-face retail sales and cash disbursements.

CARD VERIFICATION VALUE (CVV)

The CVV is a unique three-digit number encoded on the magnetic stripe of all valid Visa cards. The number is calculated by applying an algorithm to the stripe-encoded account information and is verified online at the same time a transaction is authorized. Merchants are prohibited from storing the CVV.

CARD VERIFICATION VALUE 2 (CVV2)

The CVV2 is a three-digit number that is printed on the back of all valid Visa cards either on the signature panel or beside it. Card-not-present merchants may ask the customer for the CVV2 and submit it as part of their authorization request. Merchants are prohibited from storing the CVV2.

CHARGEBACK

A formal process that allows an issuer to charge the amount of the sale back to the acquirer, because the merchant has not complied with requirements.

COMMON POINT OF PURCHASE

A merchant location or other site where data theft or replication is believed to be occurring.

FRAUDULENT APPLICATION

A submission of an application for a bankcard account where any of the personal, financial or other requested information is fraudulent.

HACKER

A person who deliberately logs on to other computers by circumventing the log-on security system. This is sometimes done to steal valuable information or to cause irreparable damage.

MAGNETIC STRIPE

The magnetic stripe is a strip of magnetic tape on the back of all bankcards. The stripe is encoded with identifying account information including the 16-digit account number and the CVV.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

A required security standard for an entity that touches or transmits Visa account information. The industry standard is adopted by Visa, MasterCard®, American Express®, Discover® and JCB.

POINT-OF-SALE (POS)

The POS is the location at which the sale or transaction takes place.

SKIMMING

The replication of account information encoded on the magnetic stripe of a valid card and its subsequent use for fraudulent transactions in which a valid authorization occurs. Full-track data is captured from a valid card and then re-encoded on a counterfeit card. The term “skimming” is also used to refer to any situation in which electronically transmitted or stored account data is replicated, and then re-encoded on counterfeit cards or used in some other way for fraudulent transactions.

VERIFIED BY VISA

Validates a cardholder’s ownership of an account in real time during an online Visa card transaction. When the cardholder clicks “buy” at the checkout of a participating online merchant, the merchant server recognizes the registered Visa card and the “Verified by Visa” screen automatically appears on the cardholder’s desktop. The cardholder enters a password to verify his or her identity and the Visa card. The issuer then confirms the cardholder’s identity.
