Data Compromise Management

Introduction

This comprehensive information summary will provide the merchant with the necessary information to understand the nature of a data compromise event as well as the necessary contact information to be used as Elavon works with the merchant to manage the data compromise event. These materials are provided by Elavon to assist the merchant in understanding the processes involved with a data compromise event. Nothing within this document should be viewed or interpreted as a modification, amendment or change to the Merchant Agreement, Terms of Service, or Merchant Operating Guide governing the merchant processing services being provided by Elavon.

Our Business

In an increasingly complex business landscape, Elavon is your global source for innovative payment solutions. Whatever a merchant needs and wherever the merchant needs it, we deliver innovative solutions to help you increase revenues, decrease costs, and sharpen your competitive edge. At Elavon, we’re elevating payments.

Contact Information

Christopher Rochelle  
Merchant Data Compromise Coordinator  
Global Association Management & Compliance  
Elavon  
7300 Chapman Highway  
Knoxville, TN 37920 USA  
Phone: 865.403.8736  
E-mail: Christopher.Rochelle@elavon.com

Chris Geron  
Vice President  
Global Association Management & Compliance  
Elavon  
7300 Chapman Highway  
Knoxville, TN 37920 USA  
Phone: 865.403.8852  
E-mail: Chris.Geron@elavon.com
Table of Contents

What is a Data Compromise Event? .......................................................... 3

What to do if Compromised ................................................................. 3

Importance of PCI/DSS Compliance ................................................... 6

Basic Outline of PCI/DSS Requirements ............................................. 6

Fines, Penalties and other Costs Resulting from a Data Compromise Event ......... 7

Education and Prevention ................................................................... 10

Glossary .............................................................................................. 16
What is a Data Compromise Event?

Simply stated, a data compromise event is an unauthorized and illegal theft of data. A central target for a data compromise event is often credit or debit card information which a perpetrator will typically re-sell or use in the production and presenting of counterfeit cards. There are three basic types of data compromise events:

1. **Physical Theft**

   Stealing receipts, hardware or other documentation which contains card data

2. **Skimming**

   Theft of card information used in an otherwise legitimate transaction
   
   - Typically an “inside job” by a dishonest employee of a legitimate merchant
   - The thief can procure a victim’s card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store a victim’s card magnetic stripe information

3. **Systemic Intrusion**

   Utilizing malicious, unauthorized and illegal means to obtain electronic access to payment processing systems or storage mediums, often referred to as hacking

What to do if Compromised

**Step 1 - Immediate containment**

- Do NOT access or alter compromised systems (i.e., do not log on at all to the machine and change passwords, and do not log in as ROOT)
- Isolate compromised systems(s) from the network (i.e., unplug network cable). Do not turn the compromised system(s) off.
- Preserve all merchant logs and electronic evidence
- Make a record of all action taken, who took the action and the date and time of such action
- If using a wireless network and a compromise is suspected, disable the wireless network
- Monitor all systems with cardholder data for possible threats or issues
Data Compromise Management

Step 2 – Alert all necessary parties immediately

- Merchant internal security group
- Elavon:
  - 865.403.8736 (Christopher Rochelle)
  - 865.403.8852 (Chris Geron)
- Law enforcement
- Merchant to check applicable state laws for possible notification to Cardholders

Step 3 – Follow-up with Elavon

Elavon will be sending the merchant a questionnaire either by e-mail or facsimile which must be completed and returned to Elavon within 3 calendar days. This information may be forwarded by Elavon to the Card Schemes as part of the investigation process.

The merchant will need to provide Elavon with the transaction information that was possibly involved in the data compromise within 7 calendar days so that the information can be provided to the Card Schemes. Elavon will assist with determining what information must be reported.

Step 4 – Determination of need for independent forensic investigation

The Card Scheme(s), in consultation with Elavon, will determine whether an independent forensic investigation will be required. Approved forensic investigations may be required to:

- Assess a compromised entity’s computing environment to identify relevant sources of electronic evidence
- Assess all external connectivity points within each location involved
- Acquire electronic evidence from compromised entity’s host and network based systems
- Forensically examine electronic evidence to find cardholder data and establish an understanding of how a compromise may have occurred
- Verify cardholder data is no longer at risk and/or has been removed from the environment
- Present forensic investigation findings to the relevant parties involved in the incident
What does it mean if I am required to get a forensic review?

If it is determined by either the Card Scheme(s) or Elavon that a forensic review is required, the merchant will need to contact the PCI Forensic Investigator (PFI) listed on the PCI Security Standards website at https://www.pcisecuritystandards.org that have been approved by the Card Schemes.

- Determine which PFI best meets the merchant needs
- Have a signed agreement within 72 hours of the merchant being notified that a forensic review is required
- Provide Elavon with the name of the PFI and the date they will be on site at the merchant location(s)

Please keep in mind that the forensic review is the responsibility of the merchant and the contract is between the merchant and the PFI.

Step 5 – Merchant to ensure all PCI/DSS requirements are met

All merchants are expected to be compliant with applicable PCI/DSS guidelines. PCI/DSS is a set of comprehensive requirements for enhancing payment account data security and was developed by the founding payment brands of the PCI Security Standards Council (PCI/SSC), including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., to help facilitate the broad adoption of consistent data security measures on a global basis. PCI/DSS is a multifaceted security standard that includes requirements for:

- Security management
- Policies
- Procedures
- Network Architecture
- Software design

Step 6 - Demonstrate PCI/DSS compliance to the Card Schemes

Once the merchant meets the appropriate requirements for PCI/DSS compliance, Elavon will assist the merchant in demonstrating full compliance to the Card Schemes.

Merchant point of contact at Elavon will be Christopher Rochelle who can be contacted at 865.403.8736 or via e-mail at Christopher.Rochelle@elavon.com.

Summarized below are the steps that need to be completed to demonstrate full PCI/DSS Compliance to the Card Schemes:

- Upgrade to a validated payment application (if applicable).

For a list of PABP-compliant payment applications please visit https://www.pcisecuritystandards.org/approved_companies_providers/index.php
Data Compromise Management

- Confirmation of passing quarterly network scans (if applicable).
  - The quarterly network scan can be completed by any of the approved scanning vendors located at the following website: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)
- Complete a fully compliant PCI/SSC Self-Assessment Questionnaire (A, B, C, or D).
  - Annual PCI Self-Assessment Questionnaire is located at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)
- Complete the Attestation of Compliance included with the Self-Assessment Questionnaire.

Importance of PCI/DSS Compliance

Meeting all the requirements of PCI/DSS is critical in protecting sensitive card data. With full compliance, merchants are less likely to have customer information compromised and stolen. The reputation of the merchant in the business community is at risk. Also, when compliant with PCI/DSS, merchants may receive reduced Card Scheme fines should a data compromise event occur.

Basic Outline of PCI/DSS Requirements

Build and Maintain a Secure Network

- **Requirement 1**: Install and maintain a firewall configuration to protect cardholder data
- **Requirement 2**: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- **Requirement 3**: Protect stored cardholder data
- **Requirement 4**: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- **Requirement 5**: Use and regularly update anti-virus software
- **Requirement 6**: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- **Requirement 7**: Restrict access to cardholder data by business need-to-know
- **Requirement 8**: Assign a unique ID to each person with computer access
- **Requirement 9**: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
Data Compromise Management

Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Fines, Penalties and other Costs Resulting from a Data Compromise Event

Every piece of cardholder account information that passes through the payment system is vital to business operation. Without proper safeguards in place, this information can be extremely vulnerable to internal and external compromise which can often lead to fraud, counterfeiting and identity theft. By failing to comply with mandated security requirements, merchants not only fail to meet their obligations to the payment system, but can cause significant financial losses due to fraud and other operational costs involved in managing a data compromise event.

When it has been determined by a Card Scheme that a merchant was the source of a data compromise, there are several costs, fines and/or penalties for which the compromised entity may be responsible. These fall into three major categories:

1. Changes and updates to merchant systems, programs and procedures
2. Card Scheme fines
3. Responsibility for the subsequent fraud and other costs

Changes and updates to merchant systems, programs and procedures

As part of the investigation process, key remediation initiatives will be recommended by either Elavon or the PCI Forensic Investigator (if a forensic investigation is required). These key remediation initiatives will be based on merchant point of sale network and other system vulnerabilities identified in the investigation process. Failure to follow the remediation guidelines can result in further cardholder fraud losses and other fines and penalties.

As part of this investigation it is possible the merchant may have to make significant changes to merchant system and/or the programs the merchant uses. These changes may be
required to become PCI/DSS compliant. These changes are the sole responsibility of the merchant and are done at the merchant's cost.

Card Scheme Fines

There are several types of fines a merchant can be liable for as a result of a data compromise. Each Card Scheme has their own fines and process for administering such fines. The fines are generally levied as a result of the merchant's improper storage of prohibited data, failing to safeguard their customer's card information and non-compliance with PCI/DSS. They can also levy case management fees that are based on the number of cards determined to have been possibly at risk. The amount of the fines may vary. The fine process is controlled by the Card Scheme, not Elavon.

Responsibility for Subsequent fraud and other costs

In addition to the Card Scheme fines, a merchant may be held responsible for the counterfeit fraud losses and other costs incurred by the card issuing banks in the form of fines from MasterCard and Visa. MasterCard can levy fines under their Account Data Compromise (ADC) program. These fines are broken down into Operational Reimbursement (OR) and Fraud Recovery (FR). Visa can levy fines under their Global Compromised Account Recovery (GCAR) program which are broken down into Incremental Counterfeit Fraud and Operating Expenses.

Flow chart for the compromised of data and subsequent fraud use
ADC

What is ADC?

Account Data Compromise (ADC) program is a MasterCard program which allows issuers to recover a portion of their magnetic-stripe counterfeit fraud losses and operating expenses. This program may be initiated by MasterCard when a merchant has experienced a data compromise event.

How does a data compromise event qualify for ADC?

This program may be initiated by MasterCard when there is an Account Data Compromise (ADC) event that has a minimum of 10,000 at-risk accounts. MasterCard reserves the right to invoke OR if fewer than 10,000 accounts are put at risk.

What does it mean if I qualify for ADC?

Could receive an assessment with either or both of the following two categories:

- Operational Reimbursement (OR) - allows issuers to recover a portion of their operating expenses such as the reissuance of the possibly compromised cards as determined by MasterCard.
- Fraud Recovery (FR) - allows issuers to recover a portion of the counterfeit fraud caused by an account data compromise.

MasterCard evaluates the totality of all of the circumstances involved in a data compromise event as well as the subsequent investigation results, merchant cooperation and other factors in determining the merchant’s financial responsibility for ADC fines.

GCAR

What is GCAR?

The Global Compromised Account Recovery (GCAR) program is a Visa program which allows issuers to recover a portion of their magnetic-stripe counterfeit fraud losses and operating expenses. This program may be initiated by Visa when a merchant has experienced a data compromise event and the causal factor in that event was the merchant’s violation of the Payment Card Industry Data Security Standard (PCI/DSS).

How does a data compromise event qualify for a GCAR?

If a merchant experiences violation involving magnetic-stripe data storage and a minimum of 15,000 eligible Visa account numbers which resulted in $150,000 or more in reported counterfeit fraud, the merchant will qualify for a GCAR liability assessment.
What does it mean if I qualify for a GCAR?

Could receive an assessment with either or both of the following two categories:

- Incremental Counterfeit Fraud - Baseline calculated at issuer BIN level, Includes counterfeit fraud reported up to $3,000 per account and PIN counterfeit fraud included
- Operating Expenses - $2.50 per eligible account for non-expired accounts

Visa evaluates the totality of all of the circumstances involved in a data compromise event as well as the subsequent investigation results, merchant cooperation and other factors in determining the merchant’s financial responsibility for GCAR fines.

NOTE: Visa and MasterCard evaluate the totality of all of the circumstances involved in a data compromise event as well as the subsequent investigation results, merchant cooperation and other factors in determining the merchant’s financial responsibility for fines.

Education and Prevention

One of the central targets for a data compromise event is credit or debit card information which a perpetrator will typically re-sell or use in the production and presenting of counterfeit cards. There are four primary means in which data compromise events are identified. In each of these four events, communication will be sent to the Card Scheme(s) who may then work with Elavon and the merchant in managing the data compromise event.

1. Issuer Monitoring
   Issuing banks, as part of their ongoing fraud monitoring, will assess trends based on reported fraudulent activity, particularly POS 90 (Swiped) fraudulent activity. When a common point of purchase or “CPP” is identified, the issuing bank may notify the Card Scheme who will in turn, notify the acquirer who sponsors the CPP merchant.

2. Law Enforcement Investigation
   Specific law enforcement agencies may investigate the theft of stolen credit card data as well as dissemination of stolen credit card data. This is done in an effort to arrest and assist in prosecution of various criminals and the members of criminal enterprise organizations. During these investigations, law enforcement agencies will notify the Card Scheme of their findings.

3. Merchant Self Reporting
   As part of ongoing PCI/DSS compliance initiatives, merchants will monitor internal activity to identify potential data breaches. If discovered, merchants should notify Elavon, which will then be communicated to the Card Networks.

4. Elavon Monitoring
   As an Acquirer, Elavon will monitor certain suspect activity as it relates to merchant processing. When a suspected or confirmed data breach is identified, Elavon will notify the Card Schemes of findings as well as begin the required response actions as outlined by the Card Scheme rules.
Data Compromise Management

Law Enforcement Investigation

Merchant Self Reporting

Card Networks

Issuing Bank Monitoring

Elavon Monitoring
Process Flow

The following flowchart provides a high level summary of each of the entities involved in identifying and managing a data compromise event. In this example, a data compromise event has occurred at a merchant location. The summary includes collection of compromise data by the issuing bank, notification to the Card Schemes, notification to the Acquirer and subsequent notification to the merchant regarding the data compromise event.

- **Issuing Bank**
  - Track counterfeit credit card usage
  - Monitor to determine any commonalities in the origin of the counterfeit transactions
  - The origin or “Common Point of Purchase” is identified and reported to the Card Networks

- **Merchant**
  - Upon identification of a data compromise event, merchant contacts with a QRH for forensic investigation and implementation of remediation steps as identified by QRH

- **Elavon**
  - Works with the merchant to:
    - Identify full scope of the data compromise
    - Contain the data compromise
    - Report all compromised cards to Card Networks

- **Validate the information from the issuer**
- **Determine initial scope of the data compromise**
- **Send notification to Elavon**
Intrusion Methodology

There are multiple methods of intrusion which may allow a perpetrator to gain unauthorized access into the Point of Sale systems and storage mediums at a merchant location. The diagram below illustrates some of the more common methodologies, or “attack vectors” in use today.

SQL Injection
SQL Injection is one of the many web attack mechanisms used by hackers to steal data from organizations. It is the type of attack that takes advantage of improper coding of web applications that allows a hacker to gain access to the data held within a database.

Insecure Remote Access
Many Point-of-Sale (“POS”) vendors, resellers and integrators have introduced remote access management products into the environments of organizations that they support. The use of remote management products comes with an inherent level of risk that may create a virtual backdoor on your system.

Insecure Wireless
The unauthorized use or penetration of a wireless network. This type of intrusion is especially prevalent where a wireless network has not been properly secured.

Malicious Code Attacks
Malicious codes or malware can be programs such as viruses, worms, Trojan applications, and scripts used by intruders to gain privileged access and capture passwords or other confidential information (e.g., user account information).

Improperly Segmented Network Environment
Network segmentation is a concept that refers to the practice of splitting a network into functional segments and implementing an access control mechanism between each of the boundaries. The most common example of network segmentation is the separation between the Internet and an internal network using a firewall/router.
The Trusted Insider

Theft can take many forms. As an employer it is important to remain vigilant in monitoring employee access to credit card information. There are various methods of employee theft, such as Physical Theft, Key Stroke Logging, Skimming and Malware.

The enemy within may encompass not just employees, but vendors/contractors, non personnel (such as visitors), and any other individuals who may have legitimate reason to be physically present with point of sale equipment or point of sale storage mediums. As a merchant, it is imperative that security procedures are in place and are strictly adhered to in order to protect valuable customer information.

Suggested Security Policies

- Initiate a badge program that includes an employee picture, and color-code specific areas of access.
- Make it a policy to question anyone who doesn't have a visible ID badge.
- Escort, observe, and supervise guests for their entire visit.
- Don't allow anyone – including vendors, salespeople, etc. – to connect personal laptops (or any other computing device) to merchant network.
- Place monitors and printers away from windows and areas where unauthorized persons could easily observe them.
- Shred or otherwise destroy all sensitive information and media when it is no longer necessary to retain.
- Do not leave documents unattended at fax machines or printers.
- Do not assume systems will not be improperly accessed by unauthorized employees.
- Periodically review point of sale equipment and location for unusual activity.
Physical Theft

Involves theft of card number storage mediums including:

- Cash Registers
- Storage Discs
- Safes
- Terminals
- Receipts
- Hardware

**Skimming:**
The use of a small portable device for theft of card data. The perpetrator, who is usually in a position of processing cards, will process a card through a skimming device, which will retain the magnetic stripe on the back of a card.

**Common merchants impacted by skimming devices include:**
- Restaurants
- Gas Stations

![Handheld Skimmer](image)
Glossary

Account Number
Payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Primary Account Number

Acquirer
Bankcard association member that initiates and maintains relationships with merchants that accept payment cards

ADC
Account Data Compromise (ADC) program is a MasterCard program which allows issuers to recover a portion of their magnetic-stripe counterfeit fraud losses and operating expenses. This program may be initiated by MasterCard when a merchant has experienced a data compromise event.

AP
Access Point (example: wireless router)

Application
Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications

Approved Forensic Investigation
An investigation that is required by one of the Card Schemes or the Acquirer that is performed by a PCI Forensic Investigator (PFI) at the merchant location

Authorization
Granting of access or other rights to a user, program, or process

Backup
Duplicate copy of data made for archiving purposes or for protecting against damage or loss

Cardholder
Customer to whom a card is issued or individual authorized to use the card

Cardholder Data
Full magnetic stripe or the PAN plus any of the following: Cardholder name, Expiration date, Service Code

Card Scheme
Alternate term used to identify Visa, MasterCard, American Express and/or Discover

Card Validation Value or Code
Data element on a card’s magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand.

Compromise
Intrusion into POS or computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected
Data Compromise Management

Chargeback
A dispute usually initiated by the cardholder to their card issuing bank that questions the validity of a specific charge to their card

CPP
Common Point of Purchase is a notification issued by one or more of the card networks that identifies a merchant as a common point of use for cardholders whose card information has been compromised and used to perpetrate fraud at other merchant locations

Database
Structured format for organizing and maintaining easily retrieved information

DBA
Doing Business As. Compliance validation levels are based on transaction volume of a DBA or chain of stores (not of a corporation that owns several chains)

DNS
Domain Name System is a hierarchical naming system for computers

DSS
Data Security Standard

Encryption
Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

Firewall
Hardware, software, or both that protect resources of one network from intruders from other networks. Typically, an enterprise with an intranet that permits workers access to the wider Internet must have a firewall to prevent outsiders from accessing internal private data resources.

FR
The Fraud Recovery (FR) program is a MasterCard program which allows issuers to recover a portion of the counterfeit fraud caused by an account data compromise.

GCAR
The Global Compromised Account Recovery (GCAR) program is a Visa program which allows issuers to recover a portion of their magnetic-stripe counterfeit fraud losses and operating expenses.

Host
Main computer hardware on which computer software is resident

Hosting Provider
Offer various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of “shopping cart” options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server
HTTP
Hypertext Transfer Protocol is open-internet protocol to transfer or convey information on the World Wide Web

IDS
Intrusion Detection System is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet

IP
Internet Protocol is network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite.

IP Address
Numeric code that uniquely identifies a particular computer on the Internet

Issuing Bank
The financial institution that issued the cardholder’s credit or debit card

Key logger
Key logging is a method of capturing and recording keystrokes. The key logger captures information in real time and sends it directly to the intruder over the Internet. Additionally, newer advances provide the ability to intermittently capture screenshots from the key logged computer.

LAN
Local Area Network is a computer network covering a small area, often a building or group of buildings

Magnetic Stripe Data (Track Data)
Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data, Card Validation Value/Code, and proprietary reserved values must be purged; however, account number, expiration date, name, and service code may be extracted and retained, if needed for business.

Malicious Code Attacks
Malicious codes or malware can be programs such as viruses, worms, Trojan applications, and scripts used by intruders to gain privileged access and capture passwords or other confidential information (e.g., user account information). Malicious code attacks are usually difficult to detect because certain viruses can be designed to modify their own signatures after inflicting a system and before spreading to another. Some malicious codes can also modify audit logs to hide unauthorized activities. Examples are malware that allows interactive command shell or backdoor, packet sniffers and key logger malware

Malware
Malicious software designed to infiltrate or damage a computer system, without a merchant’s knowledge or consent

Network
Two or more computers connected together to share resources

NTP
Network Time Protocol is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-
Packet sniffers
Packet sniffing is the practice of using computer software or hardware to intercept and log traffic passing over a computer network. A packet sniffer, also known as a network analyzer or protocol analyzer, captures and interprets a stream or block of data (referred to as a “packet”) traveling over a network.

PAN
Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account, also called Account Number.

Password
A string of characters that serve as an authenticator of the user.

Patch
Quick-repair for a piece of programming when problems are identified during software product beta test or try-out period and/or after product formal release.

PCI
Payment Card Industry

Penetration
Successful act of bypassing security mechanisms and gaining access to a computer system.

Penetration Test
Security-oriented probing of computer system or network to seek-out vulnerabilities that an attacker could exploit. Beyond probing for vulnerabilities, this testing may involve actual penetration attempts. The objective of a penetration test is to detect identify vulnerabilities and suggest security improvements.

PIN
Personal Identification Number

Policy
Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures.

POS
Point Of Sale

Procedure
Descriptive narrative for a policy that includes how the policy is to be implemented.

Protocol
Data Compromise Management

Agreed-upon method of communication used within networks. Specification that describes rules and procedures that computer product should follow to perform activities on a network.

Router
Hardware or software that connects two or more networks. Functions as a sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software Routers are sometimes referred to as Gateways.

Server
Computer that providers a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP.

Service Provider
Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching of transaction data. Also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

Skimming
Term used to describe a type of fraud where an individual uses a small portable device for the theft of card data

SQL
Structured Query Language is computer language used to create, modify, and retrieve data from relational database management systems

SQL injection
Form of attack on database-driven web site. An attacker executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization’s host computers through the computer that is hosting the database.

SSID
Service Set Identifier is a name assigned to a wireless network

Transaction Data
Data related to electronic payments

Truncation
Practice of removing data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits available in the clear

Virus
Program or string of code that can replicate itself and cause modification or destruction of software or data

Vulnerability
Weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy