First Data is now fiserv.

Benefits of

Point-to-Point Encryption (P2PE) and Tokenization to Lower Data Breach Impact

Table of contents

Executive summary

Credit card payment acceptance can help increase sales by facilitating the customer payment experience. It also helps reduce order to cash processing time and friction. However, accepting credit card payments imposes data security and legal compliance responsibilities on a business. This responsibility is not only associated with ongoing administrative and data security compliance costs, but can also incur costs associated with data security breaches. Protecting cardholder data is an ongoing endeavor since every entity processing payments or storing sensitive customer data is a target of criminal activity.

This paper will provide highlights of data breaches across multiple industries, will discuss the risks associated with accepting credit card payments and will present the payment card industry recommended solutions (point-to-point encryption and tokenization) to help reduce the risk of data breach and costs associated with protecting cardholder data.

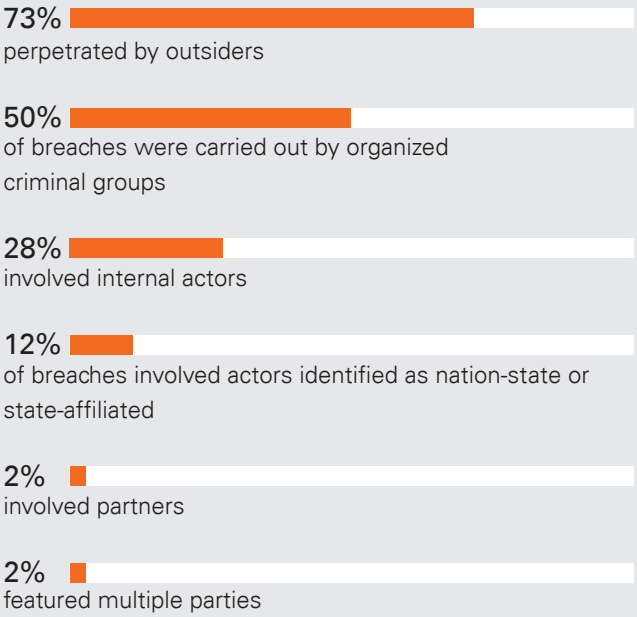
Data breaches continue to occur

Despite the proliferation and growing adaptation of secured payment processing solutions, data breach incidents continue to occur across multiple industries. Every year since 2007, Verizon has published a Data Breach Investigation Report (DBIR) to provide in-depth, multi-industry analysis of data breach incidents reported during the year. The report is generated based on analysis of thousands of real-world incidents across multiple industries and provides advice on best practices to reduce the risks of a data breach. The 2018 report includes data breach analysis for the following industries: Accommodation, administrative, agriculture, construction, education, entertainment, financial, healthcare, information, management, manufacturing, mining, other services, professional, public, real-estate, retail, trade, transportation, utilities and several small unknown businesses.

2018 Data breach incidents reported

In 2018, the Verizon DBIR reported over 53,000 data breaches (of which 2,216 were confirmed). Below is a summary of findings from the report. The data provides insight into who the perpetrators and victims are, the breach tactics utilized and what percent of the breaches were financially motivated or related to espionage.

Who's behind the breaches?



What tactics are utilized?

Source:
MG: Verizon 2018 Data Breach Investigations Report – Summary of Findings – page 5, For the confirmed data breaches:
https://www.businessinsider.com/data-breaches-2018-4#best-buy-7
https://www.pymnts.com/news/security-and-risk/2018/data-breach-user-account-card-retail-hack
https://www.idtheftcenter.org/wp-content/uploads/2018/10/2018-September-Data-Breach-Package.pdf

Who are the victims?

24%
of breaches affected healthcare organizations

15%
of breaches involved accommodation and food services

14%
were breaches of public sector entities

58%
of victims are categorized as small businesses

What are other commonalities?

76%
of breaches were financially motivated

68%
of breaches took months or longer to discover

49%
of non-POS malware was installed through malicious email

13%
of breaches were motivated by the gain of strategic advantage (espionage)

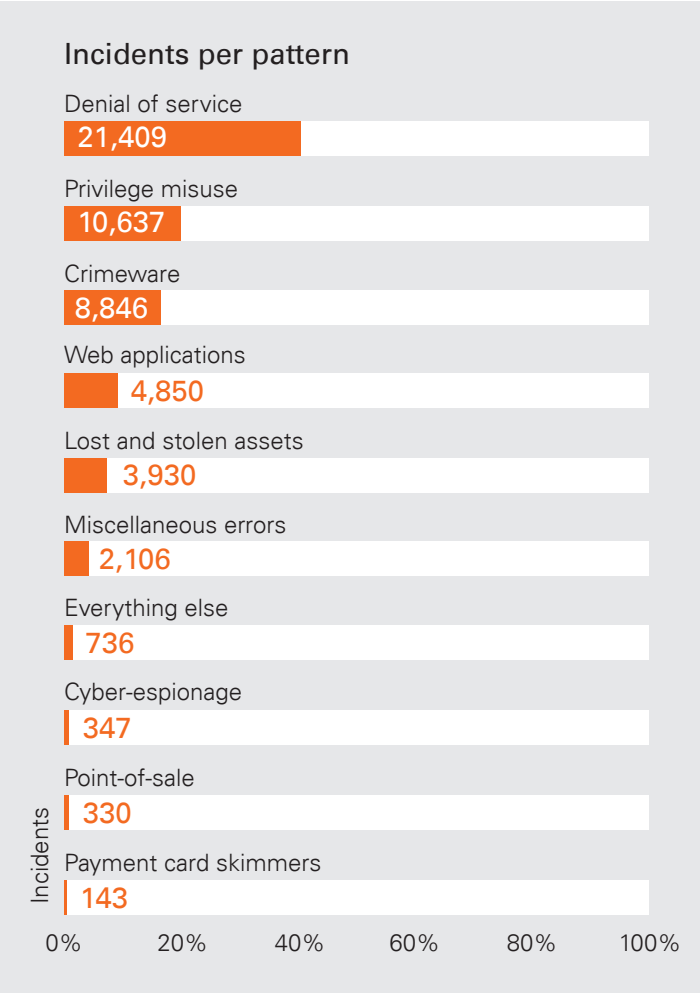
Verizon 2018 DBIR – Summary of Findings – Page 5

Important highlights from the data above include:

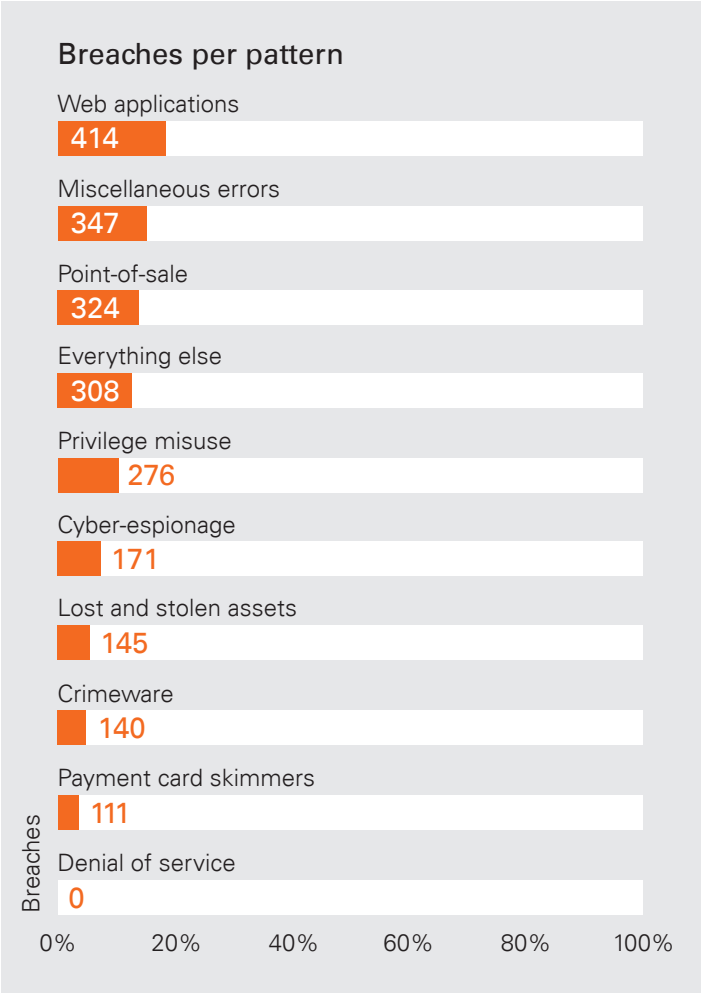
- Most of the breaches **(73%)** were perpetrated by outsiders with organized criminal groups taking the lead
- Small businesses **(58%)** and healthcare organizations **(24%)** experienced the highest percentage of breaches
- Hacking tactics were responsible for **48%** of the breaches with malware tactics being applied for **30%** of the breaches
- **49%** of the breaches involved non-POS malware installed through email
- **76%** of the breaches were financially motivated – This not only included breach of payment data but also personal and organization data
- **68%** of the breaches took months or longer to discover

Data breach patterns identified

In 2014, Verizon identified nine emerging data breach patterns from data collected over a 10-year period. The identified patterns are used to categorize security incidents and data breaches every year. With over 333,000 incidents and over 16,000 data breaches reported, the numbers reveal that 94% of security incidents and 90% of data breaches continue to fit within one of the nine patterns identified below. When compared to earlier incident reported data from previous years, the data reveals an increase of incidents related to Web Applications – accounting for the most incidents reported. This is due to businesses adopting more secured technologies such as EMV® chip credit card payment devices and data tokenization to handle card-present (CP) data. As a result, criminals are focusing breach attempts on easier targets like e-commerce and personal data systems.



Percentage and count of incidents per pattern (n=53,308)



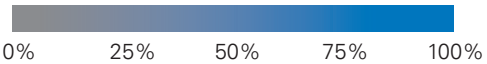
Percentage and count of breaches per pattern (n=2,216)*

*2018 Verizon 2018 DBIR – Page 22

Most prevalent incident patterns, threat actions and affected assets per industry

The table below shows the most prevalent incident patterns, threat actions and affected assets per industry identified in the 2018 report. Review the heavily shaded cells in your industry, pick a pattern and compare your industry's percent (or count) to other industries.

	Incidents									Breaches								
Patterns	Accommodation	Education	Financial	Healthcare	Information	Manufacturing	Professional	Public	Retail	Accommodation	Education	Financial	Healthcare	Information	Manufacturing	Professional	Public	Retail
Crimeware	21	19	49	154	57	284	248	5,988	26	5	2	8	14	3	8	9	9	4
Cyber-Espionage	1	12	9	24	4	82	41	120		1	12	8	9	2	22	14	77	
Denial of Service	2	151	336	1	580	74	104	703	85									
Everything Else	13	48	59	63	81	39	41	68	12	11	36	19	54	28	17	30	52	8
Lost and Stolen Assets	4	10	16	96	3	15	17	3,728	7	2	7	10	73	2		8	17	5
Miscellaneous Errors	2	16	22	181	34	3	30	1,774	11	1	15	20	172	27	2	27	50	9
Payment Card Skimmers	6		49	5		1		1	81	4		40	5				1	61
Privilege Misuse	7	7	21	138	5	22	28	10,311	11	5	3	11	128	2	8	17	51	8
Point-of-Sale (POS)	306		2	1	2		1		11	302		2	1	2		1		10
Web Applications	11	29	36	88	277	17	34	97	73	10	26	29	81	45	15	28	49	64
Actions																		
Environmental																		
Error	2	14	26	203	36	5	35	5,482	12	1	16	21	188	28	2	27	55	10
Hacking	324	210	400	139	880	150	201	925	176	316	46	50	121	62	47	66	159	77
Malware	326	35	70	185	70	359	296	6,121	71	307	14	24	27	8	24	25	90	45
Misuse	7	7	21	138	5	22	28	10,311	11	5	3	11	128	2	8	17	51	8
Physical	10	11	64	87	3	16	12	23	89	6	8	49	68	2		8	15	67
Social	14	46	63	105	69	314	257	171	10	10	41	25	56	15	18	28	96	7
Assets																		
Embedded					1	1		3										
Kiosk/Terminal	6		50	6	1	2		1	82	4		38	5				1	62
Media	5	6	25	193	2	11	12	827	16	3	5	16	183	2	1	7	36	12
Network		1	8	3	4	2	2	1	1		1		1	1				
Person	15	45	62	104	69	314	258	172	9	11	41	24	55	15	18	28	97	6
Server	338	210	419	299	920	127	202	885	189	322	42	64	245	86	42	76	105	89
User Dev	306	28	42	115	30	336	290	3,851	22	302	20	19	52	4	16	29	98	13



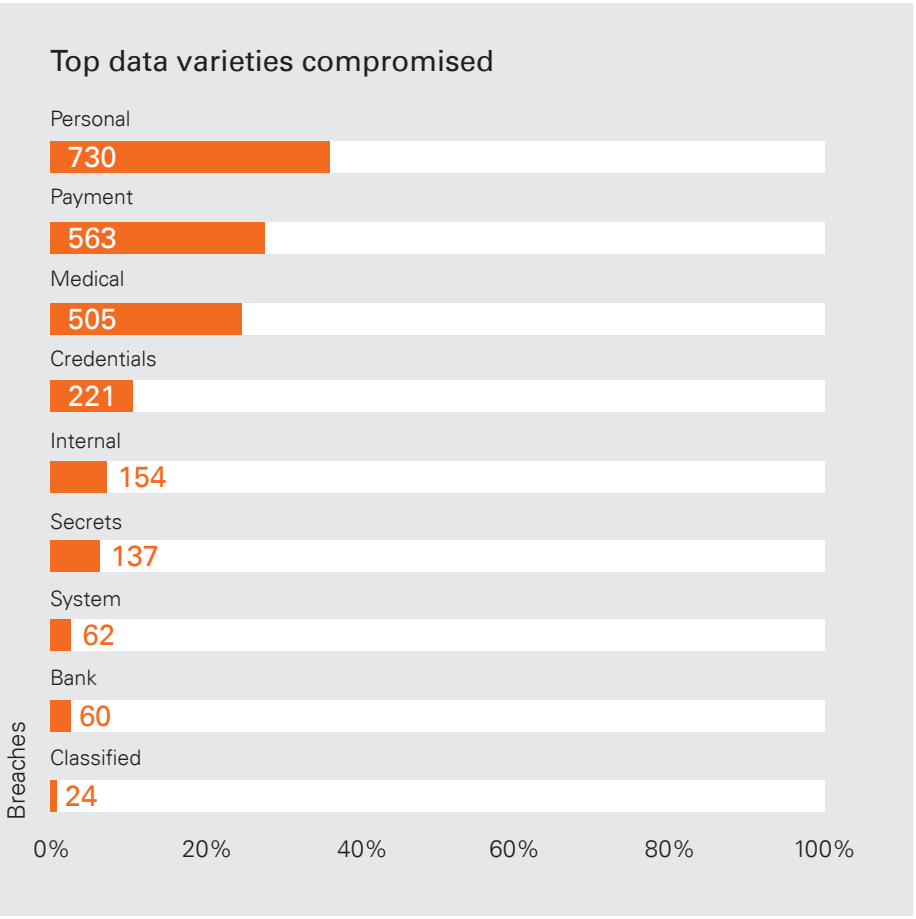
Verizon 2018 DBIR – Industry comparison (left: all security incidents, right: only confirmed data breaches) – Page 26

Highlights from the table data reported above include:

- POS systems in the Accommodation industry experienced 302 breaches
- Most of the breaches involved hacking or malware
- Web applications were targeted across all industries
- Most of the breaches occurred within physical servers and software applications (user dev)

Data variety breaches

According to the DBIR 2018 report, personal, payment and medical data were the top three among compromised data varieties associated with 2,037 data breach incidents. In 2018, there were 563 confirmed payment data breaches and 730 personal data breaches with medical and credentials data ranking in third and fourth place respectively.



Verizon 2018 DBIR - Top data varieties compromised (n=2,037)

2018 Reported data breaches

It is evident that data breaches will continue to occur year-over-year as criminals creatively find ways to exploit vulnerabilities across e-commerce, software/mobile applications and hardware. Criminals do not discriminate on company size. The 2018 data breaches listed below only represent companies that are well known to the public and made headlines. The list only represents a very small subset of all the data breaches reported in 2018.

Confirmed 2018 data breaches

The list below represents a small subset of data breaches that made 2018 headlines. The list is segmented into personal data and payment account breaches reported. Each item includes the date when the breach occurred or when reported.

Payment account data breaches

- Aadhaar – **1.1 Billion records** (March 2018 – Personal and bank account data)
- Best Buy – **Unknown number of records** (April 2018)
- British Airways – **380,000 records** (August 21, 2018–September 5, 2018)
- Cathay Pacific Airways – **9.4 Million records** (March 2018)
- Delta Airlines – **Unknown number of records** (April 2018)
- Macy's – **Unknown number of records** (April 2018)
- Orbitz – **880,000 records** (March 2018)
- Saks Fifth Avenue and Lord & Taylor – **5 Million records** (April 2018)
- Sears/K-Mart – **Approximately 100,000 records** (April 2018)

Personal account data breaches

- Adidas – **Unknown number of records** (June 2018)
- Careem – **14 Million records** (January 2018)
- Chegg – **40 Million records** (April 2018–September 2018)
- Exactis – **340 Million records** – North Americans – (June 2018)
- Facebook – **29 to 50 Million records** (July 2017–September 2018)
- Google+ – **52.5 Million records** (March 2018)
- Marriott – **500 Million records** (September 2018)
- Panera Bread – **Unknown number of records** (April 2018)
- Quora – **100 Million records** (November 2018)
- SHEIN.com – **6.42 Million records** (June 2018)
- SingHealth – **1.5 Million records** (May 2015–July 2018)
- Timehop – **21 Million records** (December 2017–July 2018)
- Ticketfly – **27 Million records** (May 2018)
- T-Mobile – **Around 2 Million records** (August 2018)
- Under Armour – **150 Million records** (March 2018)

The Verizon DBIR is one of many reputable sources that collects and reports data breach incidents every year. Knowing that cyberattacks and data breach perpetrators will continue to be a threat, organizations must be proactively alert and adapt processes, ongoing data security education and technologies to minimize the risks and effects of a data breach. Every organization is a target for a data breach. Adopting the right data breach counter-measures is the best defense that organizations can follow for minimizing the impact of a data breach.

Source:
MG: Verizon 2018 Data Breach Investigations Report – Summary of Findings – page 5, For the confirmed data breaches:
https://www.businessinsider.com/data-breaches-2018-4#best-buy-7
https://www.pymnts.com/news/security-and-risk/2018/data-breach-user-account-card-retail-hack
https://www.idtheftcenter.org/wp-content/uploads/2018/10/2018-September-Data-Breach-Package.pdf

Data security standards

Understanding the risks, processes and technologies associated with safeguarding sensitive data can be daunting. For this reason, data security standards have been established by the payment industry card brands (Visa®, Mastercard®, Discover®, Amex® and JCB) to assist merchants in navigating the complexity of protecting sensitive payment data.

The Payment Card Industry Data Security Standards (PCI DSS) were created to help any business accepting, processing, storing, or transmitting credit card data maintain a secure environment.

The PCI DSS standards are managed by the Payment Card Industry Security Standards Council (PCI SSC). The PCI Council was established in 2006 by the major payment card brands (Visa, Mastercard, Amex, Discover and JCB). The council manages the ongoing evolution of the Payment Card Industry (PCI) security standards and maintains focus on improving payment account security for credit card payments.

Businesses interested in learning about best practices or technologies for protecting sensitive data can visit the PCI Council's website for more information at (pcisecuritystandards.org/document_library).

The PCI Council's website library provides a wealth of information to assist businesses, of any size, better understand the risks of accepting payment data, become aware of security solutions to protect data, and understand their involvement and liability when handling payment data.

Risks of handling credit card or personal data

In order to identify ways to counteract a data breach, it is important to understand the risks associated with handling sensitive data (payment card data or personal data). The next section provides a comprehensive list of risks to help companies identify areas in need of data security improvements.

The list that follows is meant to help a business re-assess the level of risk they are exposed to when handling sensitive data. Any of the identified risks that are applicable to a business present an opportunity to find risk countermeasures. Not knowing if any of the risks apply to the business presents an opportunity to engage the right resources and perform risk assessment. Every organization is legally liable to protect customer sensitive data and must be aware of the risks associated with the handling of such data.

Some of the risks associated with the handling of credit card and personal data include risk of fraud, risk of data breach, risk of POS malware, risk of identity theft and risks of high PCI compliance costs.

Risks of fraud

- Using electronic payment systems (credit card terminals or POS systems) – These systems are always a target for fraud. Criminals will try to buy merchandise using counterfeit cards, use credit card skimming devices to steal card data and cyberthieves may try to intercept sensitive customer data as it transfers from your system to the payment processor.
- Bypassing credit card data validations (postal code and CVV) for credit card data provided over the phone or web applications
- Lacking a fraud prevention solution within e-commerce sites

Risks of data breach

- Accepting credit card data through encrypted or unencrypted devices, and not following a strict and persistent data security regimen to protect data
- Lacking a network perimeter security solution to guard against intrusions
- Lacking a policy for handling data security and incident response. The Lack of a data security policy with proactive policy review and data security assessment indicates data security has not been prioritized.
- Accepting credit card data in clear text through web applications
- Using credit card devices with self-managed device encryption keys while not having a secured and robust data infrastructure, proactive data security policies and device security key management programs

- Using unsecured internal data networks (weak Wi-Fi connectivity or passwords, and lacking strong network data security certificates)
- Storing sensitive data within systems without proactive system monitoring and periodic system security updates
- Overlooking human error – overlooked user access controls, user account sharing, unrestricted administrative access, unsecured data storage systems, system security out of date, user access logs not monitored periodically, staff not properly trained to handle sensitive data, or recognize criminal data extraction schemes
- Accepting or storing credit card data using unsecured channels (e.g., phone, email, fax, text)
- Storing or transmitting encrypted sensitive data with locally stored decryption keys
- Recording card data received through phone calls (e.g., call center)

Risks of POS malware

- Running an out-of-date POS software application
- Transmitting POS data in clear-text
- Providing unrestricted user POS application access
- Lacking system monitoring processes and anti-virus software for all workstations
- Configuring POS workstations in a publicly accessible network
- Running out-of-date POS workstation without system security updates
- Exposing POS systems to any user
- Using POS systems with unencrypted credit card terminals or standard keyboard for credit card data entry

Risks of identity theft

- Storing (encrypted or unencrypted) sensitive personal and cardholder data
- Lacking user access controls to sensitive data
- Lacking phishing scam training and prevention software – (Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons, by disguising as a trustworthy entity in electronic communication – e.g., email, web links)
- Lacking processes/training to counteract Social Engineering (Social Engineering is the art of manipulating people, so they give up confidential information)
- Lacking staff training to keep safeguards on sensitive information (e.g., leaving printed sensitive information in the open, not locking cabinets, unlocked computer screens and writing sensitive information on sticky notes)
- Entering credit card or personal data into websites that do not have a valid security certificate
- Providing unsecured open data networks and accepting and allowing the passing of sensitive data through unencrypted channels

Risks of high PCI compliance costs

- Using non-PCI validated payment processing technologies – incurs high recurring PCI compliance costs while subjecting a business to high data breach risks
- Lacking data security processes and technology – incurs yearly hefty compliance costs (including fines)
- Not selecting a payment gateway service provider that complies with PCI standards
- Not selecting a payment gateway service provider that focuses on reducing PCI compliance costs for the business or does not provide PCI scope reduction across multiple payment channels
- Not adopting a PCI scope reduction solution across all payment processing channels
- Receiving fines for being non-PCI compliant. Non-PCI compliant merchants may be liable for penalties imposed by merchant acquirers or the card brands. The fines will vary depending on merchant contract, merchant processing volume and type of data breach incident.

Assessing the risks for handling credit card and personal data is the first step in identifying risk countermeasures. After the risk assessment is completed, the next step is identifying the right processes and technologies to mitigate risks.

In the next section, we discuss available solutions to help organizations protect customer data while reducing costs and liabilities for the business.

Solutions to reduce credit card and personal data risks and liabilities

To help minimize the bulk of data protection risks identified, the PCI Council recommends the adoption of P2PE and tokenization as the best solutions to mitigate the risks of protecting sensitive data. A P2PE solution with tokenization helps organizations reduce the yearly recurring costs and processes associated with PCI compliance.

What is P2PE?

A P2PE solution helps organizations protect themselves and their customers from a costly data breach.

Through a combination of secure devices, applications and processes, businesses can encrypt data directly from the point of interaction (POI – e.g., through a credit card terminal during a credit card dip or swipe) until the data reaches a solution provider's secure decryption environment. This means the data isn't decipherable to anyone who might steal it during the transaction process and thus lacks value for thieves. Point-to-point encryption protects credit card data in flight through merchant systems, to help prevent it from being compromised.

Although point-to-point encryption isn't the only solution that helps protect sensitive payment data, many experts and the PCI Council rank it high. It takes more than one strategy to optimize security but implementing a P2PE solution is a good first step.

How does P2PE work?

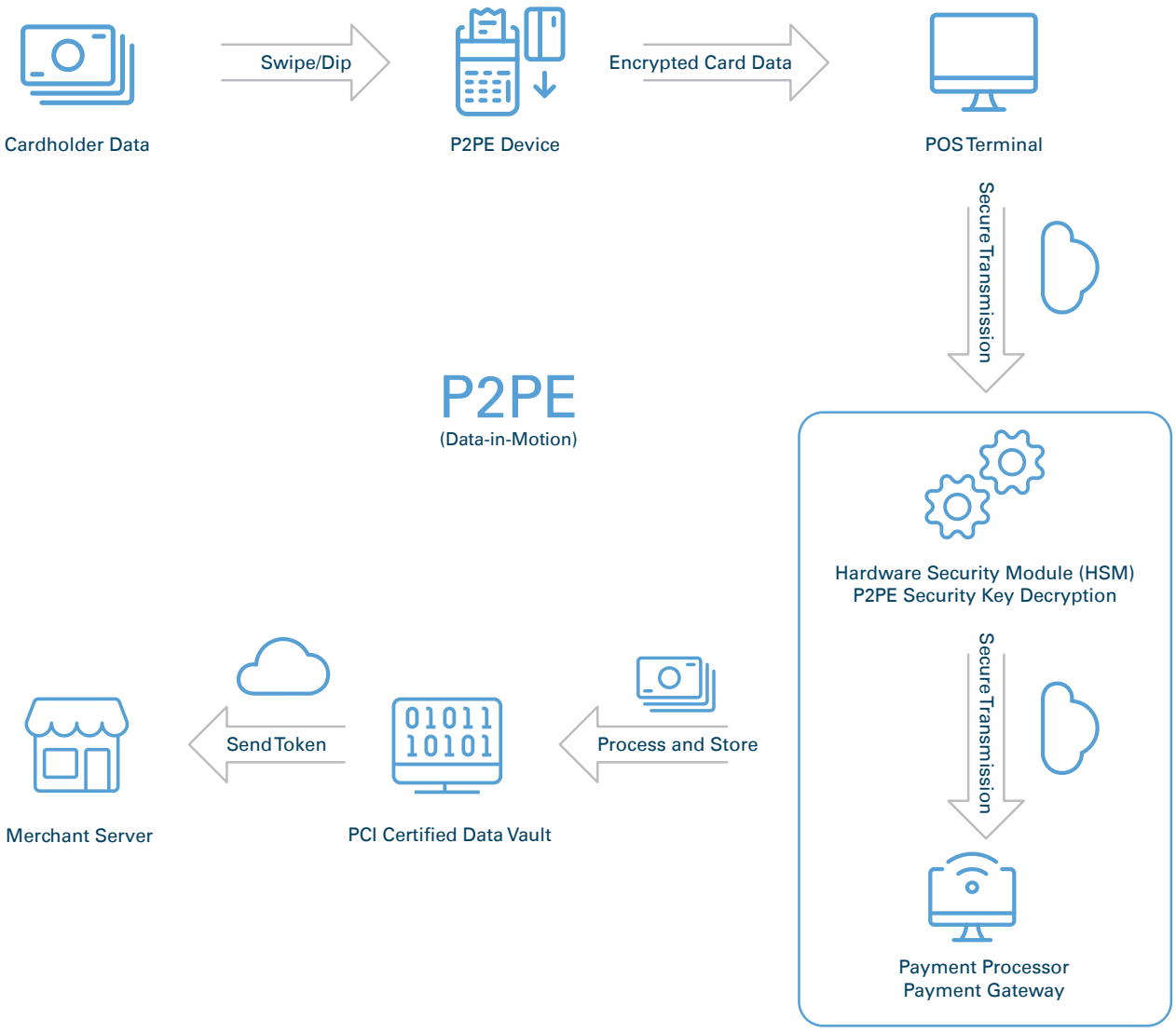
As a payment card is taken (manually keyed, swiped, tapped/contactless or dipped) through a credit card reading device POI, the device immediately encrypts the card information.
A PCI-validated P2PE solution uses very strong encryption keys (e.g., TDES-DUKPT, AES, RSA, and so on.) to encrypt payment card data as it is entered. From the POI, the encrypted data is sent to the payment gateway or processor through a secured connection (HTTPS/TLS1.2). The payment gateway or processor receives the encrypted data and uses a decryption key (generally stored within a Hardware Security Module or HSM) to retrieve the original card data. The keys for encryption and decryption are never available to anyone but the solution provider, making card data completely invisible within the merchant's environment. Because the solution provider manages the keys, the merchant never has encrypted data and the keys together, so a hacker cannot get card data from the merchant's system and data breach is avoided.

Once the data is decrypted within the secure payment processor environment, the data is passed to the credit card issuing bank for authorization. The bank processes payment transaction and provides authorization status to merchant (approved or declined), along with a credit card token the merchant can store. The generated credit card token can then be reused to submit a subsequent transaction without the need of the original credit card number. Later in this document, the "tokenization" section discusses tokenization and the benefits it provides for protecting different types of data.

Source:
https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/What-effect-does-the-use-of-a-PCI-listed-P2PE-solution-have-on-a-merchant-s-PCI-DSS-validation

P2PE solution data flow

The following diagram depicts the general data flow of a credit card transaction processed with a P2PE PCI validated solution.



PCI-validated P2PE solutions

Not all P2PE solutions are validated by the PCI Council. To reduce PCI scope, merchants must select a P2PE solution from the PCI-validated solutions listed within the PCI Council website. A P2PE solution not listed within the PCI Council's website has not met the PCI P2PE standard and will not offer reduced PCI scope for a business. Only council-listed P2PE solutions are recognized as meeting the requirements necessary for merchants to reduce the PCI scope of their cardholder data environment through use of a P2PE solution.

PCI-P2PE solution requirements

The PCI Council's P2PE Standard defines the requirements that a "solution" must meet in order to be accepted as a PCI validated P2PE solution. A solution is a complete set of hardware, software, gateway, decryption, device handling and so on. Only solutions can be validated; individual pieces of hardware such as card readers cannot be validated alone as a P2PE solution.

- A P2PE solution uses a hardware-to-hardware encryption and decryption process along with a POI device that has SRED (Secure Reading and Exchange of Data) listed as a function
- A P2PE Qualified Security Assessor (P2PE-QSA) determines whether a solution meets the P2PE standard. P2PE-QSA companies are independent third-party companies who employ assessors that have met the PCI Security Standards Council's requirements for education and experience and have passed the required P2PE-QSA exam. The PCI Security Standards Council does not validate solutions, it only sets the standards for the solution. Validation is handled by a PCI Qualified Security Assessor.
- The PCI P2PE Standard includes specific POI device requirements such as strict controls regarding shipping, receiving, tamper-evident packaging and installation
- A P2PE solution includes merchant education in the form of a P2PE Instruction Manual, which guides the merchant on the use of POI devices, storage, return for repairs and regular PCI reporting
- A P2PE solution is facilitated by a third-party solution provider
  For example, a processor, acquirer or payment gateway). The solution provider has overall responsibility for the design and implementation of a specific P2PE solution and the management of P2PE solutions for its merchant customers. The solution provider is accountable to ensure that all P2PE requirements are met, including any P2PE requirements performed by third-party organizations on behalf of the solution provider (e.g., certification authorities and key-injection facilities).

P2PE solution benefits

Merchants adopting a PCI-P2PE validated solution benefit from simplified compliance efforts, since they are subject to fewer PCI DSS requirements. This in turn can save significant time and money as PCI requirements are greatly reduced. Organizations deploying a P2PE validated solution can qualify to complete a shorter PCI Self-Assessment Questionnaire. The PCI self-assessment questionnaire can be reduced from 12 sections (SAQ-D) to four sections (P2PE-HW) and the controls are reduced from 329 questions (SAQ-D) to just 35 (P2PE-HW).

A P2PE solution also protects a business in the event of fraud, the P2PE solution provider, not the merchant, is held accountable for data loss and resulting fines that may be assessed by the card brands (that is Amex, Visa, Mastercard, Discover and JCB).

Tokenization

What is Tokenization?

Tokenization is often confused with P2PE as both solutions involve converting sensitive data into data that is useless to hackers. Tokenization and P2PE are different technologies that serve different purposes within a merchant environment.

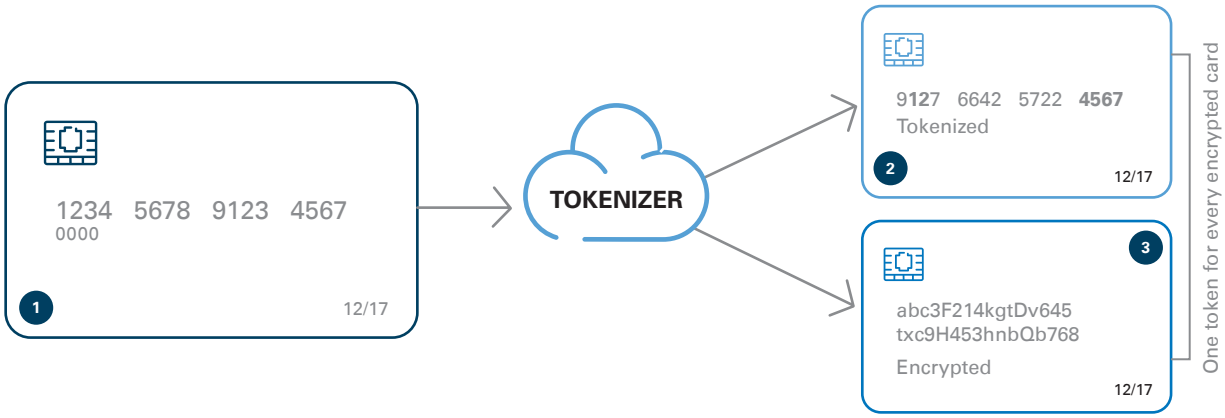
As explained previously, a P2PE solution is used to protect credit card data as the data travels from the POI to the solution provider's secured environment. A P2PE solution is generally paired with tokenization to produce a randomly generated number that represents a payment card. The token length and format varies per solution provider. This randomly generated number can then be reused by a business to process a future transaction through the solution provider's payment gateway.

The token does not contain credit card data, is not a value that can be decrypted back into the original credit card (only the solution provider can regenerate the original card number – with some exceptions where a merchant can decrypt tokens) and it cannot be used outside the solution provider's payment gateway. Credit card tokens generally reflect the last-four digits of the credit card but may also include the first two or six digits (BIN number) of the card. Because a token does not contain sensitive data, a business can store the token without the burden of ongoing PCI compliance related to storing cardholder data. We should source these statements.

Tokenization is a technology that enables the creation of data tokens for a variety of sensitive data (e.g., credit card data, SSN, email, phone, license, and so on).

The token format for each data type varies based on the data being tokenized. Tokenization solutions also provide a business the ability to detokenize sensitive data (usually not credit cards due to risk) to obtain the original data. A good tokenization/detokenization solution will provide every business with a unique set of encryption keys for the generation of tokens. Meaning, that tokens generated by a specific business cannot be used by another business. The tokens generated are for the exclusive use of a respective business. A tokenization solution allows the exchange of tokenization requests through a secure network or internet connectivity (e.g., SSL/TLS 1.2 connection).

Tokenization example



In the image above, a credit card (1) is converted to a token (2) using tokenization. The token is provided back to a merchant for storage. In this example, the generated token is a credit card token. It can be used for processing a future payment through the solution provider payment gateway. The card encrypted data (3) is maintained within the solution providers secured environment. The merchant can store the token which does not fall under PCI data scope.

Benefits of tokenization

Tokenization has been utilized for many years to mitigate the risks associated with protecting sensitive data (payment and personal data).

Tokenization provides the following benefits:

Reusable protection

Tokenization protects cardholder data at many points in the transaction lifecycle, especially post-authorization and recurring transactions once a payment card has been tokenized.

Reduces administrative and PCI compliance costs

The use of tokenization simplifies PCI compliance by reducing the scope associated with storing payment card data. Because card data is no longer being stored, in the merchant systems the amount of time and resources associated with the protection of data is reduced. This results in reduced administrative and PCI compliance costs for the business.

Devalues breached data

Tokenization removes all cardholder data stored in merchant systems and applications and replaces it with numbers that are useless to an attacker. This allows the merchant to rest easier knowing that any perpetrator would only get access to nonsensical number data in the merchant system rather than customer-sensitive Primary Account Numbers (PANs). Tokens cannot be unencrypted to generate the original credit card number.

Simplifies PCI compliance

Tokenization reduces PCI scope audits and complexity. Merchants using tokenization qualify for shorter PCI self-assessment questionnaires and can complete the PCI assessment faster.

Reduces liability

For a business handling data for European customers, tokenization can be leveraged to help comply with the General Data Protection Regulation (GDPR) and reduce financial liability for the business.

Internal data protection

Tokenization not only protects sensitive information from criminals but also minimizes internal and external data exposure to people within an organization (e.g., employees, vendors and suppliers).

Online data protection

Merchants can leverage tokenization across multiple channels (e.g., e-commerce, retail, and internal/external systems) to substantially reduce the risk of data breach and protect sensitive data.

Protects multiple data types

Tokenization can be leveraged to protect not only payment data (e.g., credit cards, bank accounts, gift cards, etc.) but also Personally Identifiable information (e.g., social security numbers, phone, email, date of birth, license data and credentials).

Summary

As data breaches continue to make headlines, alarming consumers and merchants alike, it is critical for businesses to stay informed and adopt technologies to assist with proactive data protection. Technology solutions such as Tokenization and Point-to-Point encryption can help a business protect sensitive data while reducing yearly PCI compliance administrative costs. Prioritizing and applying protective measures for payment and personal data is an ongoing endeavor that benefits customers and merchants.

Businesses that fall victim to a data breach are harmed in different ways. A data breach can result in fines from the card associations and lawsuits from government agencies, other organizations and even consumers. A data breach can harm the business reputation for a prolonged time, resulting in lost revenue, lost customer trust and customer retention. A tarnished reputation can ultimately ruin a business in some cases.

Instead of worrying about recovering from the risks associated with a data breach, businesses can adopt tokenization and P2PE solutions to help protect their assets, reputation and customers.

About Miguel Gracia

Miguel Gracia, VP of Solutions Engineering, is a senior executive with 30 years of technology experience. His expertise revolves around payment processing solutions, tokenization, Point-to-Point Encryption (P2PE) terminals, e-commerce, network security and information security within PCI guidelines.

In 2012, Miguel Gracia joined CardConnect®, which was then subsequently acquired by First Data. He supports the B2B Enterprise Payments team as a Sr. Solutions Engineer and develops product solutions within the Enterprise Gateway Integration and Support groups. Miguel has completed hundreds of payment processing integrations within the CardConnect gateway. For over 20 years, Miguel has taken lead roles during the design, testing, deployment and management of secured data networks, PCI data compliance processes and information systems and IT departments supporting customers in diverse payment processing environments.

Miguel Gracia has an undergraduate degree in computer science from the New Jersey City University and a Master of Science in IT Management from the Stevens Institute of Technology.

For more information, please contact us at 630.429.9845 or B2Bpayments@firstdata.com

FirstData.com

First Data is now fiserv.