



# P2PE, Security & Mobile Payments

Miguel Gracia & David Natelson  
April 15, 2019

**First Data.**

© 2019 First Data Corporation. All rights reserved. The First Data name, logo and related trademarks and service marks are owned by First Data Corporation and are registered or used in the U.S. and many foreign countries. All trademarks, service marks, and trade names referenced in this material are the property of their respective owners.

0



## Agenda

- › Data Breaches Continue
- › Data Security Standards
- › Risks of Handling Payment and Sensitive Data
- › Point-to-Point-Encryption
- › Tokenization
- › Mobile Payments (David Natelson)
- › Q & A

**First Data.**

1

## Data Breaches Continue to Occur

### Verizon Data Breach Investigation Report (DBIR) – Reputable resource

- Collects and reports data breach incident data (since 2007)
- Data is collected across multiple industries

### 2018 Verizon DBIR Report

- Over 53,000 (of which 2, 216 were confirmed) data breaches
- 73% of breaches were perpetrated by outsiders
- Small businesses and Healthcare organizations experienced the highest percent of breaches
- 58% of the breached victims were small businesses
- 48% of the breaches were related to hacking with malware
- 49% of the breaches involved non-POS malware installed via email
- 76% of the breaches were financially motivated
- 68% of the breaches took months or longer to discover



### <sup>1</sup>Security Breach State Level Legislation

- NC was one of the first states to pass laws in 2005 (Senate Bill 1048) now N.C. Gen. Stat §§ 75-61, 75-65
  - Notification to NC State Consumer Protection Bureau for breaches affecting more than 1,000 people
  - <https://www.ncdoj.gov/getdoc/81eda50e-8feb-4764-adca-b5c47f211612/Report-a-Security-Breach.aspx>
- 50 States have had security breach notification bills
- States with newly enacted legislation in 2018 - AL, AR, CA, CO, CT, HI, IA, IL, KY, LA, MD, MA, MI, MO, NE, NH, NM, NY, OH, OR, SC, SD, UT, WA, DC

<sup>2</sup> <sup>1</sup>Source: <http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx>

First Data.

2

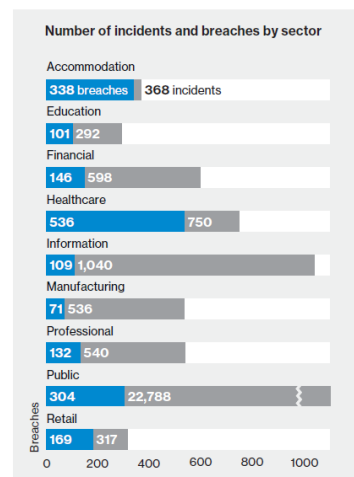
## Data Breaches Continue to Occur

### Data Breach Patterns Identified

- Nine emerging data breach patterns identified from data collected over a 10-year period
- Patterns:**
  - Denial of Service** (massive traffic load which disables web application access)
  - Privilege Misuse** (e.g., too many user accounts with access to sensitive data)
  - CrimeWare** (e.g., malware, keylogger, viruses)
  - Web applications** (unsecured web applications)
  - Lost and Stolen assets** (lost computers/data)
  - Miscellaneous Errors** (human error – e.g., writing down sensitive data, unsecured workstations)
  - Cyber-Espionage**
  - Point of Sale**
  - Payment Card Skimmers**
- Note:** 333,000 incidents and over 16,000 data breaches reported reveal that 94% of security incidents and 90% of data breaches fit within one of the 9 patterns.

### The <sup>2</sup>2018 DBIR report shows that:

- Point-of-Sale 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



<sup>2</sup>Source: <https://enterprise.verizon.com/resources/reports/dbir/>

First Data.

3

3

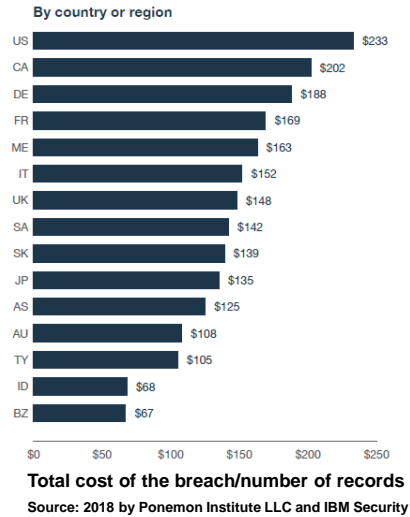
# 2018 Data Breaches Reported by the Media

## Payment Account Data Breaches

- Saks Fifth Avenue and Lord & Taylor - 5 million records (April 2018)
- British Airways - 380,000 records (August 21, 2018 — September 5, 2018)
- Orbitz - 880,000 records (March 2018)
- Best Buy - unknown number of records (April 2018)
- Delta Airlines - unknown number of records (April 2018)
- Macy's - unknown number of records (April 2018)
- Sears/K-Mart - around 100,000 records (April 2018)

## Personal Account Data Breaches

- Panera Bread - unknown number of records (April 2018)
- Ticketfly - 27 million records (May 2018)
- Google+ - 52.5 million records (March 2018)
- Quora - 100 million records (November 2018)
- Under Armour 150 million records (March 2018)
- T-Mobile - around 2 million records (August 2018)
- Adidas - unknown number of records (June 2018)
- Facebook – 29 to 50 million records (July 2017 - September 2018)
- Marriot - 500 million records (September 2018)
- 4 ▪ Aadhar – 1.1b citizens of India (March 2018), India's government ID biometric database



First Data.

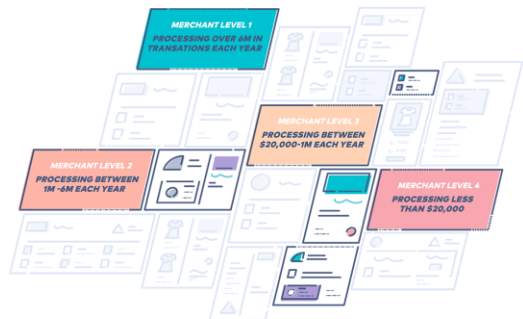
# Data Security Standards

## Payment Card Industry Data Security Standards (PCI DSS)

- A set of data security standards for protecting sensitive data
- Define the do's and don'ts when protecting payment card data
- Established by the Card Brands (Visa, Mastercard, Discover, Amex and JCB)
- Assist merchants in navigating the complexity of protecting sensitive payment data

## Payment Card Industry Security Standards Council (PCI SSC)

- Established by the card brands in 2006
- Manages PCI DSS standards
- Manages the ongoing evolution of the PCI security standards
- Maintains focus on improving payment account security for credit card payments.
- To learn more visit Council's website at <https://www.pcisecuritystandards.org>



First Data.

## Risks of Handling Credit Card or Personal Data

### Risks of Fraud

- Bypassing payment data validations (postal code and CVV)
- Lacking a fraud prevention solution within Ecommerce sites

### Risks of Data Breach

- Using unencrypted devices when accepting sensitive data
- Not monitoring network access against intrusions
- Lacking a process for handling data security incidents
- Accepting credit card data in clear text via web applications
- Using credit card devices with self-managed device encryption keys
- Using unsecured data networks or channels (e.g., weak Wi-Fi connectivity or passwords, taking card data over the phone)
- Storing unencrypted payment data within systems
- Overlooking human error – e.g., user account sharing, unrestricted access, untrained staff handling payment data
- Storing or transmitting encrypted sensitive data with locally stored decryption keys
- Recording card data received via phone calls (call center)

6

First Data.

6

## Risks of Handling Credit Card or Personal Data

### Risks of POS Malware

- Running an out-of-date POS software application
- Transmitting POS data in clear-text
- Lacking anti-virus software for all workstations
- Configuring POS workstations in a publicly accessible network
- Exposing POS systems to any user

### Risks of Identity Theft

- Storing (encrypted or unencrypted) sensitive personal data
- Lacking Phishing scam training and prevention software - (The attempt to obtain sensitive data by disguising as a trustworthy entity via email or web links)
- Lacking processes to counteract Social Engineering (The art of manipulating people, so they give up confidential information)
- Lacking staff training to keep safeguards on sensitive information
- Entering sensitive data into websites that do not have a valid security certificate
- Providing unsecured open data networks that allow passing sensitive data via unencrypted channels

7

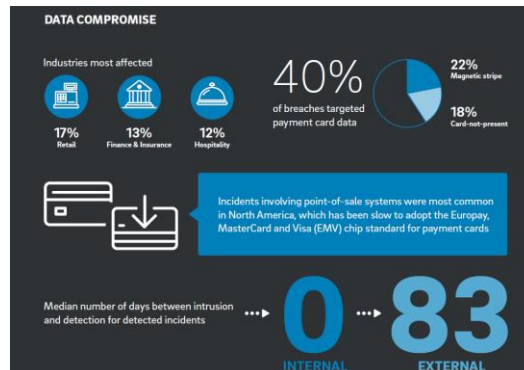
First Data.

7

## Risks of Handling Credit Card or Personal Data

### Risks of High PCI Compliance Costs

- Using non-PCI validated payment processing technologies (incurs high PCI costs while exposing a business to data breach risk)
- Lacking data security processes and technology (incurs yearly hefty compliance costs - including fines up to \$500k)
- Not selecting a payment gateway service provider that complies with PCI standards
- Not adopting a PCI scope reduction solution across all payment processing channels.



8

Source: 2018 Trustwave Global Security Report <https://www2.trustwave.com/GlobalSecurityReport.html>

First Data.

8

## Point-to-Point Encryption (P2PE)

### What is Point-to-Point Encryption?

- A combination of secure devices, applications and processes to encrypt and protect data throughout the entire transaction
- Uses hardware-to-hardware encryption and decryption process
- Makes card data completely invisible within the merchant's environment.
- Solution includes merchant education in the form of a P2PE Instruction Manual (PIM)
- Encrypted data isn't decipherable to anyone who might steal it during the transaction process
- Helps organizations protect themselves and their customers from a costly data breach
- Is ranked as a high security solution by the PCI council and security experts

### PCI-Validated P2PE Solution

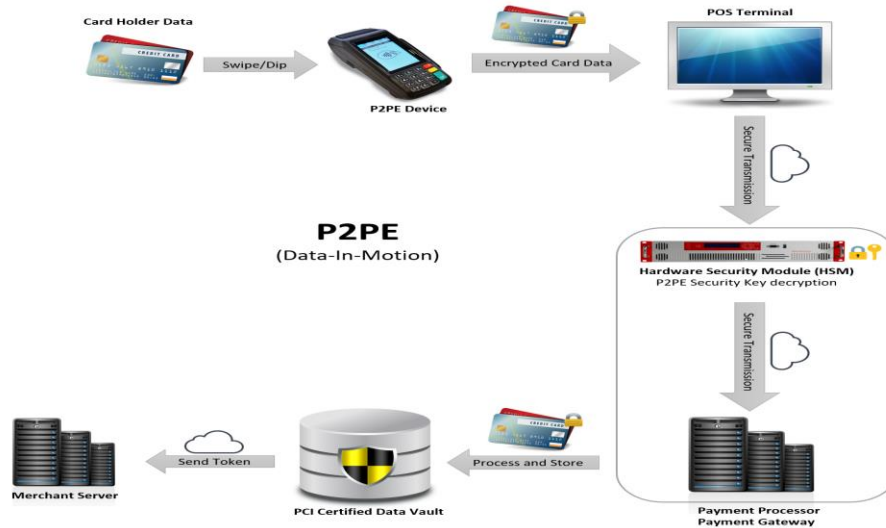
- Not all P2PE solutions are validated by the PCI Council.
- To reduce PCI scope, merchants must select a P2PE solution listed within the PCI Council website
- Non PCI listed solutions have not met the PCI P2PE standards and will not offer reduced PCI scope for a business
- Only Council-listed P2PE solutions are recognized as meeting the requirements

9

First Data.

9

## Point-to-Point Encryption (P2PE)



10

First Data.

10

## Point-to-Point Encryption (P2PE)

### How Does P2PE Work?

- Immediately encrypts data at the point-of-interaction (POI) - as the data is keyed, dipped or swiped
- Uses strong encryption keys (e.g., TDES-DUKPT, AES, RSA, etc.)
- From the POI, the data is sent to the solution provider via a secured connection (HTTPS/TLS1.2)
- Solution provider uses a decryption key (stored within a Hardware Security Module or HSM) to retrieve the original card data
- Encryption/Decryption keys are never available to anyone but the solution provider
- Shifts data protection liability to the solution provider
- Solution provider passes the data the credit card issuing bank for authorization
- Once the transaction is processed, merchant receives the authorization status (approved/declined) along with a credit card token from the solution provider
- The merchant can store the token and re-use it for subsequent transactions. No need for retaining the original card data.



11

First Data.

11

## Point-to-Point Encryption (P2PE)

### PCI Council Validated P2PE Solution Benefits

- Simplifies PCI compliance efforts - fewer PCI DSS requirements.
- Saves time and money as PCI requirements are greatly reduced.
- Shorter PCI Self-Assessment questionnaire (P2PE-HW – 35 controls)
- Protects a business in the event of fraud, the P2PE Solution Provider, not the merchant, is held accountable for data loss and any resulting fines

12

First Data.

12

## Tokenization

### What is Tokenization?

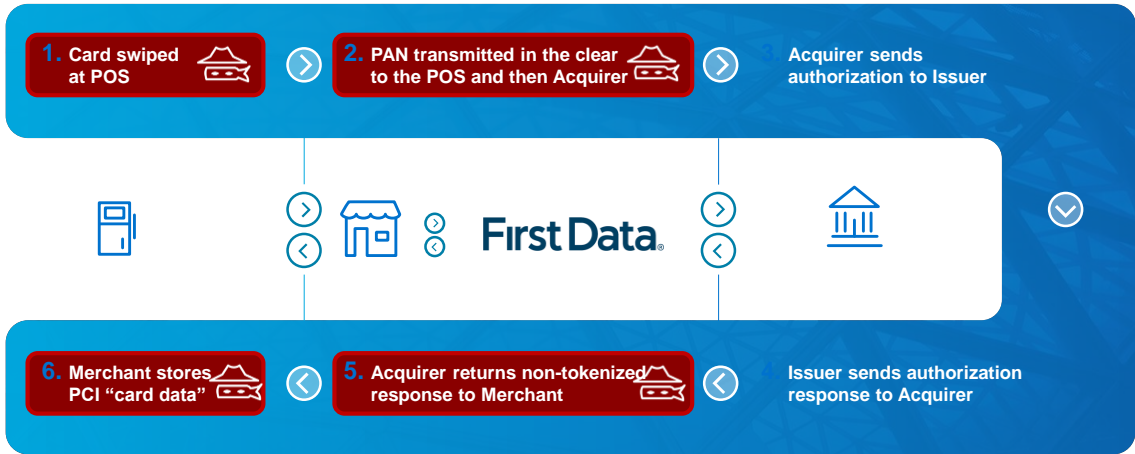
- A technology that enables the creation of data tokens for a variety of sensitive data (credit card data, SSN, email, phone, license, etc.)
- Provide the ability to detokenize sensitive data (usually not credit cards due to risk) to obtain the original data
- Is based on a unique set of encryption keys for the generation of tokens
- Exclusive tokens generated for a specific business cannot be used by another business
- Allows the exchange of tokenization requests via secure connectivity (e.g., SSL/TLS 1.2 connection)
- Often confused with point-to-point encryption (P2PE), as both solutions involve converting sensitive data into data that is useless to hackers
- P2PE is paired with tokenization to produce a randomly generated number that represents a payment card
- The token length and format vary per solution provider
- This randomly generated number can be reused to process future transactions via the solution provider's payment gateway
- A token does not contain credit card data, is not a value that can be decrypted back into the original credit card
- Credit card tokens generally reflect the last 4 digits of the credit card but may also include the first 2 or 6 digits (BIN number) of the card.
- A business can store the token without the burden of on-going PCI compliance related to storing card holder data

13

First Data.

13

# Where threats lie



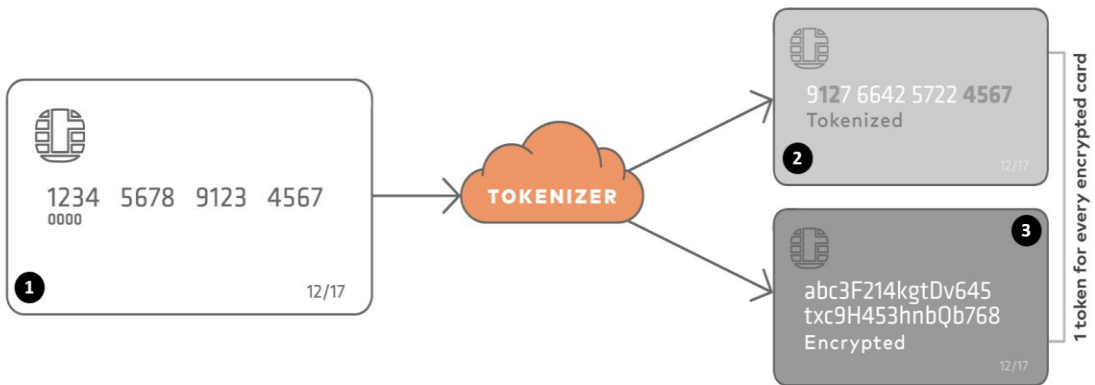
14

First Data.

14

# Tokenization

## Tokenization Example



15

First Data.




15





# Summary – current PCI Validated P2PE Solutions from First Data

[https://www.pcisecuritystandards.org/assessors\\_and\\_solutions/point\\_to\\_point\\_encryption\\_solutions](https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions)

COMPANY	P2PE VERSION	P2PE ASSESSORS	REGIONS SERVED	REASSESSMENT DATE
<b>CardConnect, LLC</b>				
Solution Name: CardSecure P2PE				
Reference #: 2017-00113.004	P2PE v2.0	SecurityMetrics, Inc.	North America	20 Jul 2020
<p><b>Description Provided by Vendor:</b> The CardSecure® P2PE Solution by CardConnect is an end-to-end encryption and PCI-validated solution. Merchants who use this solution could significantly reduce their PCI Scope while simultaneously increasing their security. Compatible with any sales channel, this solution ensures that data is encrypted upon read rendering it useless to any malware that may be downstream. The CardSecure P2PE Solution ensures that no merchant has access to encryption keys, and that CardConnect manages them in a PCI-compliant manner. This solution substantially reduces merchant risk and is future-proofed with EMV and NFC functionality. CardConnect is a leading provider of payment technology and processing services, with customers ranging in size from Fortune 50 corporations to corner stores and small businesses. Securing cardholder data is a cornerstone of our offering, and it provides a substantial value proposition for our merchants because it reduces their PCI Scope.</p>				
 <p>ISC Touch 250 Features: EMV, NFC, Apple Pay, Touchscreen, Signature Capture</p> <p>IPP350/320 Features: EMV, NFC, Apple Pay</p>				
<b>First Data Merchant Services</b>				
Solution Name: First Data TransArmor P2PE Solution - Ingenico On-Guard				
Reference #: 2018-00541.001	P2PE v2.0	Sysnet Limited, dba Sysnet Global Solutions	North America	4 Jan 2022
<p><b>Description Provided by Vendor:</b> First Data's TransArmor P2PE Solution is part of a comprehensive, multi-layered security solution covering all PCI card brands. The TransArmor P2PE Solution, with Ingenico's On Guard encryption, allows integrators tremendous implementation flexibility using legacy integrations; and can reduce the scope of merchant data subject to PCI compliance. This cost-effective solution is available for most verticals including retail, restaurant, QSR and healthcare.</p>				
 <p>Ingenico iSC250 Touch, iSC480, iPP320, iPP350, iPP310</p>				
<b>Clover Network Inc, a wholly-owned subsidiary of First Data Corporation</b>				
Solution Name: Clover				
Reference #: 2017-00893.001	P2PE v2.0	Payment Software Company (PSC)	Worldwide	30 Oct 2020
<p><b>Description Provided by Vendor:</b> Clover's payment processing solutions let you accept credit cards, EMV chip and contactless payments from customers, safely and securely. Clover's P2PE solution combines the security of Clover devices with TransArmor encryption. TransArmor protects payment card data in Clover devices throughout the entire transaction process since data is encrypted from the moment you dip, swipe, tap, or sign.</p>				
 <p>Clover Mini Accept swipe, EMV chip and NFC payments right out of the</p>				

Look for more brands and devices in 2019...

First Data.

