



# Security and the Payments Environment

Protecting You and Your Customers' Data

Craig Tieken

Vice President, TransArmor product offering

May 18, 2010

**Dial-In: 1-866-551-1530 Pin code: 3967081#**

# Welcome

## Speakers:

### **Craig Tieken**

Vice President  
First Data Corporation

### **Robert McMillon**

Director of Solution Development  
RSA

### **Nick Holland**

Senior Analyst  
Aite Group, LLC

# Retail use of electronic payments is growing

If it seems like you have more electronic transactions these days, you do.

- In the U.S. in 2009, there were
  - 20.2 billion credit transactions totaling \$1.76 trillion
  - 36.2 billion debit or prepaid card transactions totaling \$1.6 trillion
- 73% of U.S. consumers used a credit card in the past year
- 80% of U.S. consumers own a debit card

Sources: Federal Reserve Bank of Boston, January 2010 and Nilson Report, February 2010

# Significant breaches of payments data

Company	Reported	Records breached
CardSystems Solutions	May 2005	40 million
TJX Companies	January 2007	94 million
Dave & Buster's	August 2007	Unknown
Hannaford Brothers	March 2008	4.2 million
Heartland Payment Systems	January 2009	130 million

Breaches involving payment card data far outnumbered breaches of any other data type in 2008. Nearly 80% of the incidents investigated by the Verizon Business RISK Team involved the loss of sensitive cardholder data.

# Regulations are putting pressure on merchants

**PCI DSS** – Payment Card Industry Data Security Standards imposed on all merchants by card brands. “Comply or risk losing ability to accept payment cards.”

**State breach laws** – Forty six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.

**International laws** – Data breach notification and disclosure laws are emerging around the globe.

# What is at Risk for Merchants

Business risks from data exposure

<b>Risk</b>	<b>Outcome</b>
<b>Losses from fraud</b>	Banks and payment processors may reclaim losses they sustain as a result of a merchant's data breach
<b>Expenses for credit monitoring</b>	Customers whose data is stolen may be entitled to credit monitoring for at least a year
<b>Fines by card brands</b>	Card companies may issue fines for PCI DSS noncompliance and prohibited data storage practices
<b>Remediation costs</b>	Capital expenditures may be necessary to replace or upgrade compromised hardware, software, applications and communications
<b>Brand damage</b>	Public reporting of a breach often is required by law, making it impossible to escape widespread bad publicity and loss of confidence in merchant's brand
<b>Expense of forensic exam and in-depth PCI audit</b>	A forensic investigation could take months with very high costs
<b>Potential lawsuits</b>	From customers, financial institutions, ISOs, payment processors, card brands, state attorneys general, and more
<b>Drop in market cap</b>	When damages are high, a merchant's stock value and overall market capitalization can drop

# What this means for merchants

More investment in security and compliance...

- National Retail Federation reports its members collectively spent more than \$1 billion on PCI DSS compliance as of June 2009

...For little added value

- Security assessments and measures do little to increase sales
- However, compromised security can result in lost business

43% of consumers who have been victimized by fraud avoid certain merchants where they believe their data could be compromised again.

# The new “arms race”

Merchants must adapt and layer security methods as thieves become increasingly sophisticated in attack methods.

Data thieves are becoming laser-focused in their approach, targeting specific companies for the precise data they can quickly monetize.

Source: Symantec Global Internet Security Threat Report: Trends for 2009

# Cost effective ways to fight back

- Build layers of security around cardholder data when it must be present
- Render the data useless to thieves when possible
- Do not store cardholder data in your environment

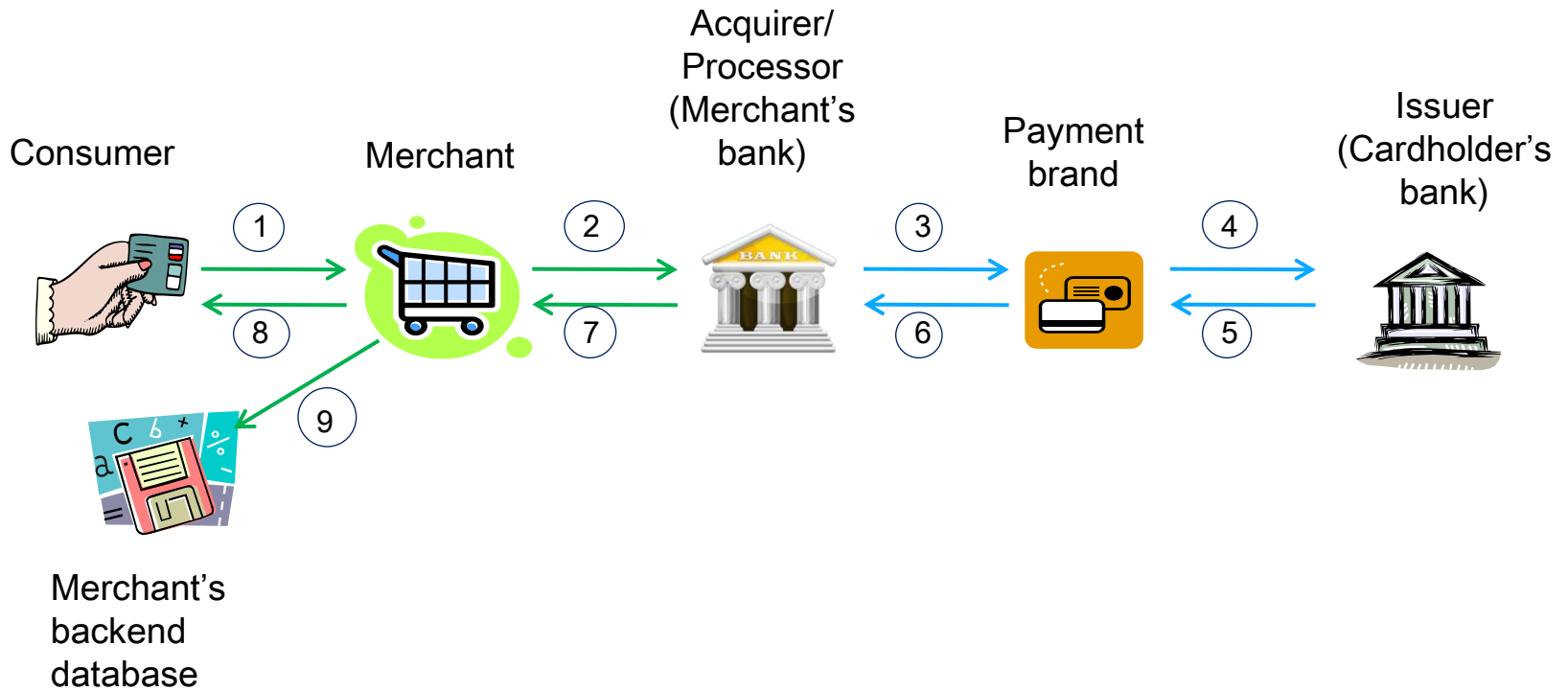
# The states of data

**At rest** – Cardholder data is being aggregated or stored somewhere

**In transit** – Cardholder data is moving along a communications channel as it passes from one entity (such as a merchant) to another (such as an acquirer/processor)

**In use** – Cardholder data is being used by an active application

# The Payments Processing Chain

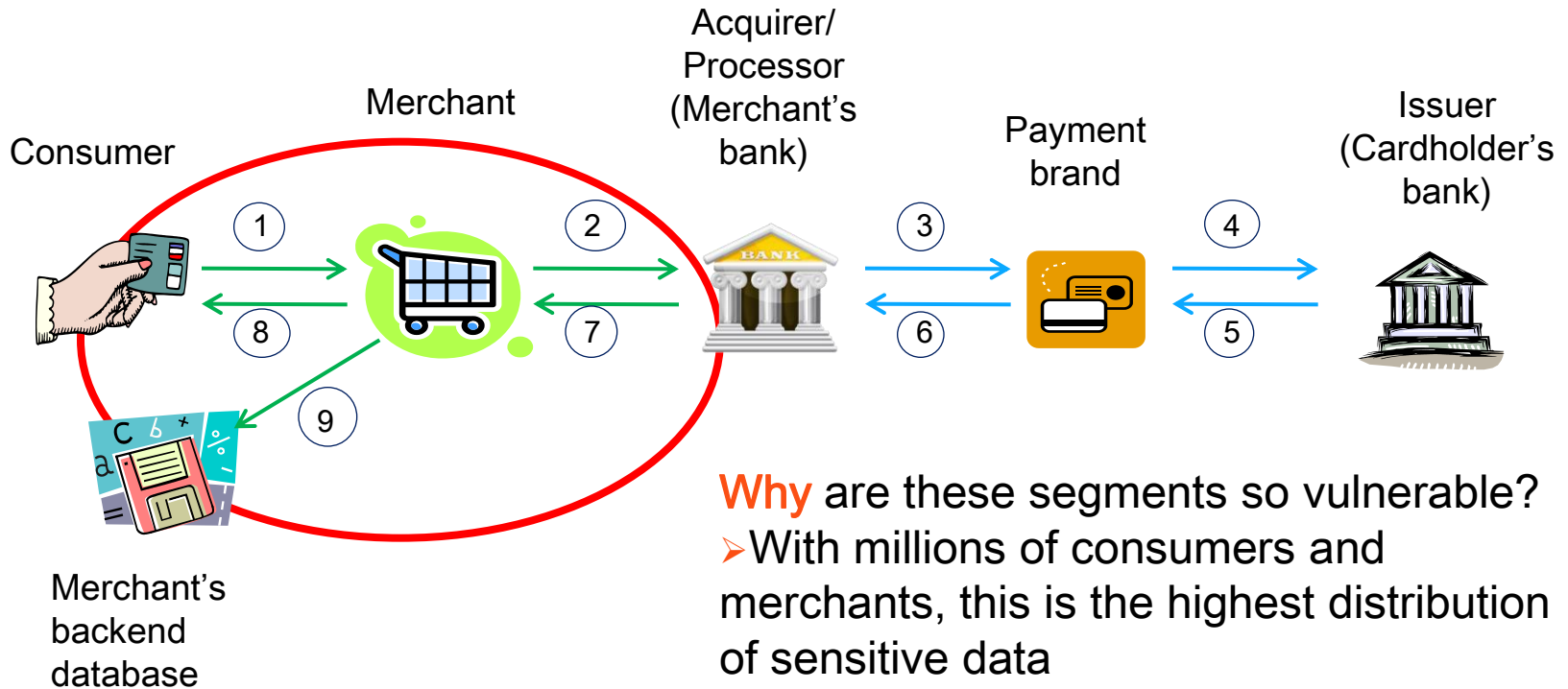




For Merchants

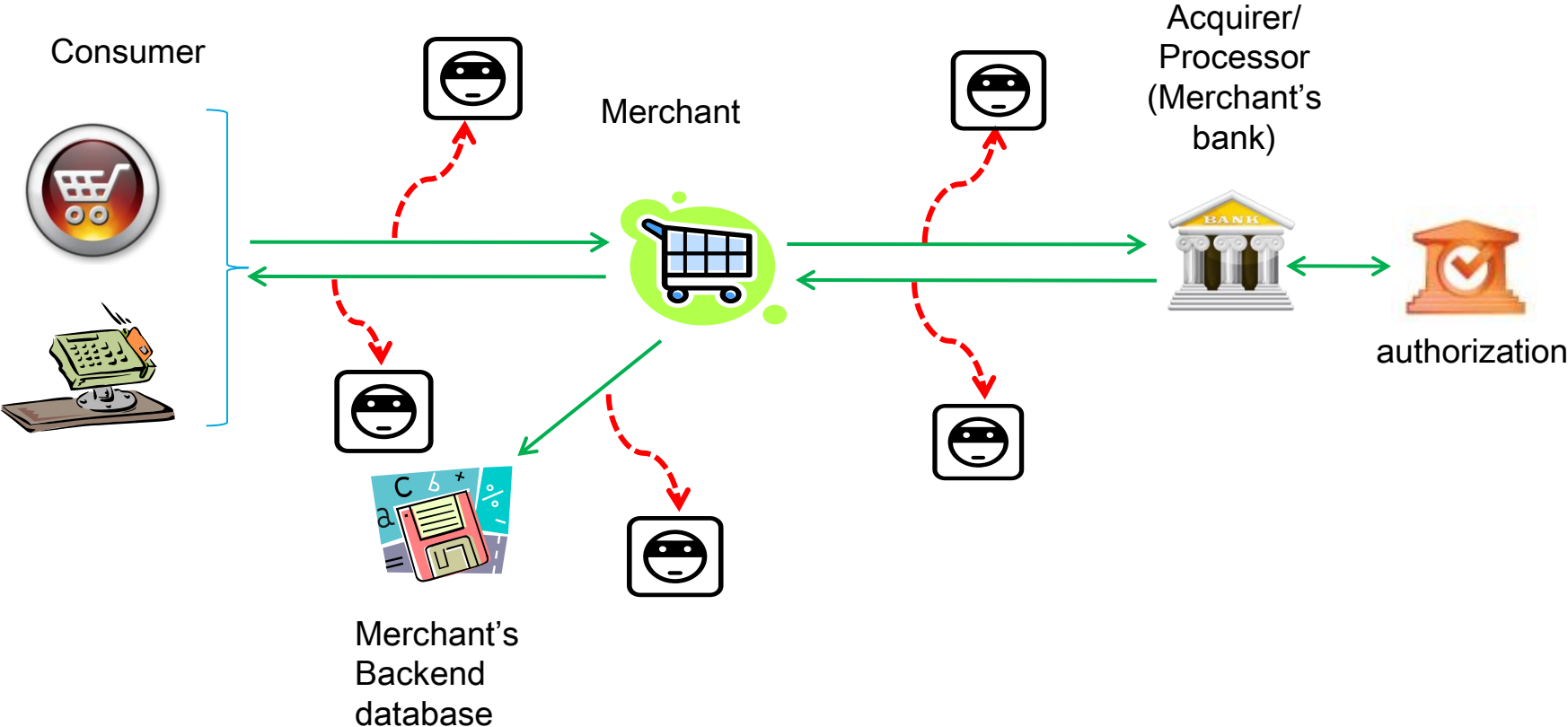
# Major Points of Vulnerability

# The most vulnerable segments of the Transaction Cycle



- Why** are these segments so vulnerable?
- With millions of consumers and merchants, this is the highest distribution of sensitive data
  - Security measures vary greatly by merchant and some are still in early stages

# Data is vulnerable in transit



# Data is vulnerable at rest

## Merchant stores data after transaction

- On a POS server or store server until end of day
- In a central database for ancillary purposes
- Moved to various endpoints where security is lax (e.g., spreadsheets)

*Every place where cardholder data is stored is part of the CDE and subject to PCI audit!*

# Technology solutions address areas of greatest vulnerability and need

➤ End-to-end encryption (E2EE)



➤ Tokenization



Both technologies render cardholder data useless to thieves.

# End-to-end encryption

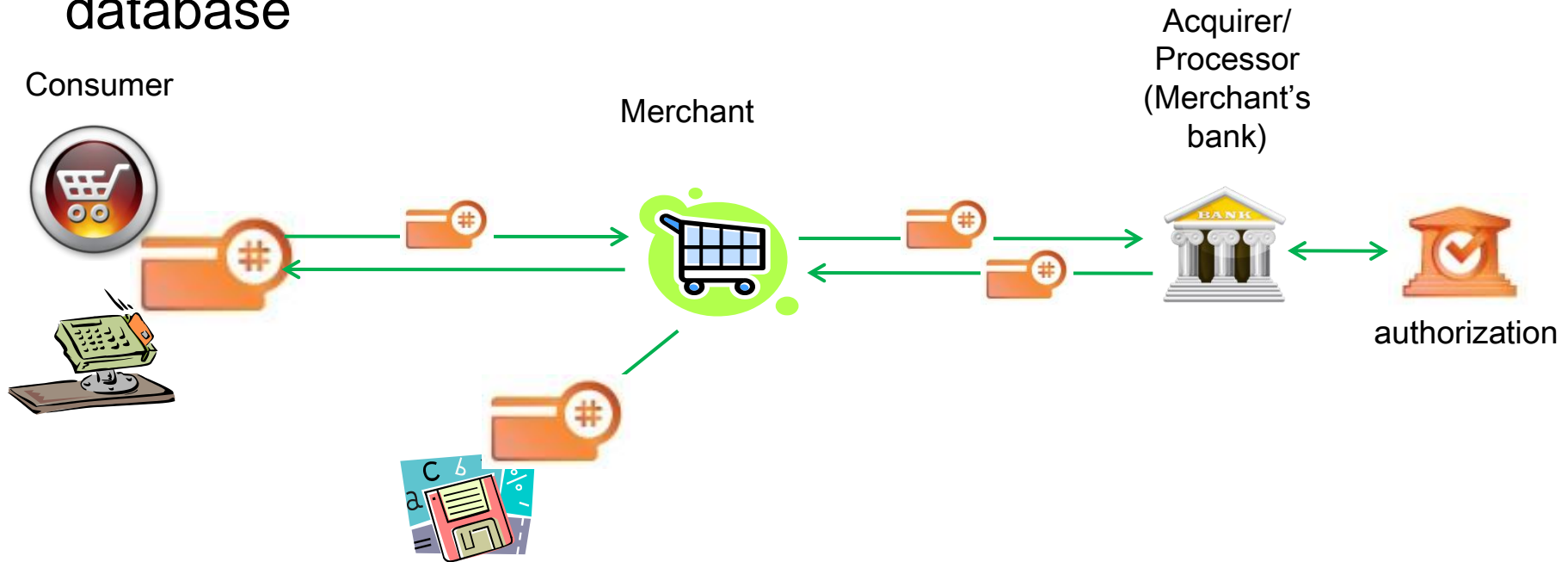


- Encryption uses algorithmic methods that encode plain text (such as a cardholder number) into a non-readable form called ciphertext.
- E2EE encrypts data at the time the consumer presents it (card swipe or entry into e-commerce app) and allows it to remain encrypted until acquirer/processor receives it.
- Merchant possesses key to encrypt data; acquirer/processor possesses key to decrypt data before authorization

# Where encryption fits

**Data in transit** – from moment card is swiped or data is entered, to store server, to acquirer/processor

**Data at rest** – in store server or merchant backend database



# Problems that encryption solves



- Sending cardholder data in clear text as it moves upstream to acquirer/processor
- Storing cardholder data in clear text for ancillary use

*But...* it doesn't significantly reduce scope and cost of PCI compliance and assessment



# Tokenization

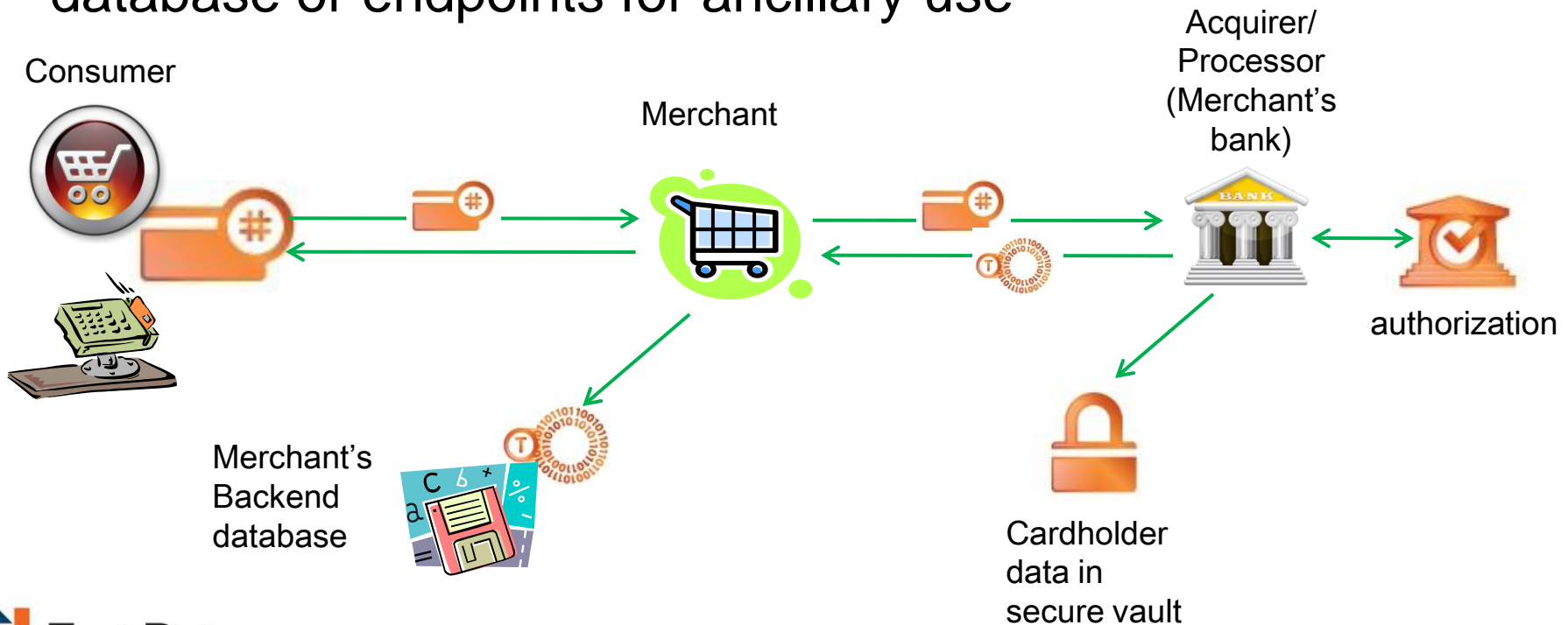
- After a transaction is authorized, tokenization will substitute random data for sensitive data and then store the sensitive data in a secure vault
- Merchant receives auth code and tokenized data for ancillary use



# Where tokenization fits

**Data in transit** – After transaction is approved and auth is sent back to merchant

**Data at rest** – In store server or merchant backend database or endpoints for ancillary use





# Problems that tokenization solves

- Eliminates having live cardholder data in storage or in use for ancillary applications
- Reduces scope and cost of PCI compliance and assessment because cardholder data is no longer present

# Benefits of using encryption and tokenization together

- Encryption adds another layer of security for data
  - If encrypted data is breached, it isn't usable
- Tokenization takes cardholder data out of merchant's environment
  - If tokenized data is breached, it isn't usable
  - Reduces scope and cost of PCI compliance and assessments
- Merchants can use tokenized data in existing applications without modifying them
- Both encryption and tokenization can be added with minimal effort and costs

