BREAK SERVICE

Continental Breakfast – Breakfast Breads and Fruit (Beginning at 7:30 am)
Coffee (Regular and Decaf)
Soft Drinks
Afternoon Snacks – Cookie Assortment

BUFFET LUNCH MENU

Catered by: Barbecue Lodge

Entrees:
Chopped Pork Barbecue
Fried Chicken

Vegetables:
Green Beans
Boiled Potatoes
Macaroni and Cheese
Cole Slaw

Breads:
Hushpuppies and Rolls

Dessert:
Banana Pudding and Apple Cobbler

Beverages:
Iced Tea, Iced Water, and Lemonade

REGISTRATION

Registration fee: $30.00
(Check-in begins at 7:30 am)

Registration Deadline: April 15, 2014

Further registration details can be found at:
http://www.osc.nc.gov/cpe/courses.html

eCommerce
from paper to electronic

Location
3512 Bush Street
Raleigh, NC 27609-7509

Mailing Address
1410 Mail Service Center
Raleigh, NC 27699-1410

Website
www.osc.nc.gov

OFFICE OF THE STATE CONTROLLER

2014 eCommerce
Conference

April 30, 2014

The McKimmon
Conference & Training Center
N.C. State University

1101 Gorman Street
Raleigh, NC 27606
919-515-2277

Course Overview

Objective:

To provide information on the Office of the State Controller's (OSC) Statewide eCommerce Program. Participants will learn how to better use services offered through the eCommerce Program and learn about new services being considered. Relevant issues pertaining to Electronic Funds Transfer (EFT) and merchant card processing will be discussed. The various vendors supporting eCommerce will participate. Focus will be on assisting agencies in identifying how they can gain business process efficiencies in eCommerce.

A Special "Thank You" to Our Conference Sponsors:

AMERICAN EXPRESS

Bank of America

DISCOVER

First Data. beyond the transaction

Trustwave®

State Services Attending:

- Office of the State Controller/ Office of Information Technology Services: Common Payment Service
- Department of the Secretary of State: E-Notary

Course Level: Basic

Teaching Method: Lecture

Advance Preparation: None

CPE Credit: Up to 7 hours

Prerequisites: Employed by a state agency, university, community college or a local unit of government that participates in the State's eCommerce Program.

AGENDA

7:30-8:10........................Registration/ Vendor Networking

8:10-8:20...…………….....….Welcome
James G. Dolan, Office of the State Controller

8:20-9:05………Emerging Trends in eCommerce
Alan Kelly, Rhonda Kirk and Stephanie Spencer, First Data

9:05-9:50……….Technology to Take Your Business to the Next Level: Payment Solutions to Engage and Protect Customers
Rip Creekmore, American Express

9:50-10:20……………………Break/ Vendor Networking

10:20-11:05......................Securing the Transaction: An Overview of Point-to-Point (P2P) Encryption
Michael Garvin, Symantec

11:05-11:50……….............Electronic Funds Transfer (EFT)/ Prepaid Cards
Doris Dixon, Shannon Okine and Luke Harris Bank of America/Department of the State Treasurer and Office of the State Controller

11:50-1:05……..….……...……Lunch/ Vendor Networking

AGENDA (CONT.)

1:05-2:05………..PCI DSS Security Awareness Training
Shawn Ryan, AGIO

2:05-2:50…The Cost of Compromise
Special Agent Stanley Crowder, U. S. Secret Service

2:50-3:35...…………...……….Break/ Vendor Networking

3:35-4:35.........……Panel Discussion: "eCommerce in Government – A Look at the Opportunities and Challenges"
Moderator: *Maurice Ferrell, UNC School of Government – Center for Public Technology*

Panel Participants: *Carl Pickney, Department of Transportation; Dee Bowling, East Carolina University; Rick Owens, Pitt Community College and Bill Greeves, Wake County Government*

4:35-4:40….….Conference Wrap-up
Amber Young, Office of the State Controller

Note: Click the following link for additional information about the Office of the State Controller, the sponsor and developer of this program.

Office of the State Controller
eCommerce Conference

From Paper to Electronic

McKimmon Center – Raleigh, North Carolina – April 30, 2014

7:30 – 8:10 am	**Registration/Vendor Networking**
8:10 – 8:20 am	**Welcome** *Jim Dolan, Acting State Controller*
8:20 – 9:05 am	**Emerging Trends in eCommerce** *First Data: Alan Kelly, Rhonda Kirk and Stephanie Spencer*
9:05 – 9:50 am	**Technology to Take Your Business to the Next Level: Payment Solutions to Engage and Protect Customers** *American Express: Rip Creekmore*
9:50 – 10:20 am	**Break/Vendor Networking**
10:20 – 11:05 am	**Securing the Transaction: An Overview of Point-to-Point (P2P) Encryption** *Symantec: Michael Garvin*
11:05 – 11:50 pm	**Electronic Funds Transfer (EFT)/Prepaid Cards** *Bank of America: Doris Dixon; Department of State Treasurer: Shannon Okine; Office of the State Controller: Luke Harris*
11:50 – 1:05 pm	**Lunch/Vendor Networking**
1:05 – 2:05 pm	**PCI Data Security Standards – Security Awareness Training** *AGIO: Shawn Ryan*
2:05 – 2:50 pm	**The Cost of Compromise** *U. S. Secret Service: Special Agent Stanley Crowder*
2:50 – 3:35pm	**Break/Vendor Networking**
3:35 – 4:35 pm	**Panel Discussion – eCommerce in Government – "A Look at the Opportunities and Challenges"** *UNC School of Government: Maurice Ferrell – Moderator* *Panel – Department of Transportation: Carl Pickney; East Carolina University: Dee Bowling; Pitt Community College: Rick Owens; Wake County Government: Bill Greeves*
4:35 – 4:40 pm	**Conference Wrap-up**

Office of the State Controller
2014 E-Commerce Conference
Speaker Biographies

Emerging Trends in E-Commerce

Alan Kelly – Alan is in his 10th year at First Data. He began his tenure working as a successful TeleCheck Account Executive. He later joined First Data's Learning Organization as a Level-1 and Level-2 Trainer. Alan was promoted to Sales Director and Regional Sales Director of First Data's Revenue Sharing Alliance and managed the North Texas and Oklahoma regional sales team. In May 20007, Alan joint the Solution Consultant team where he currently serves as a trusted product advisor for the Mid Market Client Acquiring Portfolio at First Data.

Rhonda Kirk – Rhonda is a Relationship Manager for the Mid Market segment at First Data, a position she has held for the past five years. She joined Telecheck in 1987 which was acquired by First Data and has over 27 years of financial expertise in the areas of merchant services. Rhonda holds a B.S. degree from Appalachian State University majoring in Business.

Stephanie Spencer – Stephanie is a Director of Relationship Management for the Mid Market segment at First Data. She joined First Data in 2007 and has over 10 years of banking experience in the areas of merchant services and treasury management. She holds a B.S. degree from Ohio State University majoring in communications.

Technology to Take Your Business to the Next Level: Payment Solutions to Engage and Protect Customers

Rip Creekmore – Rip is a Senior Client Manager, Government and Public Education, Southeast Region, and has been with American Express Merchant Services for 25 years, including 14 years providing information, consultation, and service to merchant customers in the State & Local Government and Public Education sectors. Rip was instrumental in working with the Office of the State Controller to establish the current State Master Agreement for American Express Card Acceptance, and he is the primary contact for the State & Local Government and Public Education entities in North Carolina. Rip is responsible for ensuring customer satisfaction, consulting on payment services and trends, and delivering value to both existing and future merchant partners.

Securing the Transaction: An Overview of Point-to-Point (P2P) Encryption

Michael Garvin – Michael is a seasoned IT professional with over 20 years of experience in information security and compliance, IT architecture and management, and systems administration. He started with Symantec in 2006 and is currently a member of the Information Security Services (ISS) team. His responsibilities include live fire cyber security training, skills development, and practice through cyber exercises and ranges, Symantec's CyberWar Games and Cyber Readiness Challenge events, and product management in related areas. Michael has actively participated in the PCI community, including the PCI SSC's Scoping and EMV SIGs and the annual Community meetings. He has also been involved in the security metrics community, local ISSA chapter, and with lectures at NC State University School of Business. Michael has spoken at the 2011 Internet Summit, has co-presented in a CSO Online webcast on PCI 2.0, and has spoken at Symantec's Vision conference. Among his certifications, Michael is a Certified Information System Security Professional (CISSP), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT), and hold the Certificate of Cloud Security Knowledge (CCSK) as an Early Adopter.

Electronic Funds Transfer (EFT)/Prepaid Cards

Doris Dixon – Doris Dixon works for Bank of America Merrill Lynch and is a senior prepaid card product specialist on the North American Product Sales team, focusing on government prepaid card solutions. Within this team under Global Treasury Solutions, she is responsible for working with government client teams to identify and understand client needs and strategically develop prepaid card solutions to meet those needs. Doris joined Bank of American Merrill Lynch in 2001 as a marketing product manager, responsible for the marketing of all Commercial Prepaid and Payroll Card products. Over the years, she has also served as a senior product manager for the bank's CashPay Visa Payroll Card, Commercial Prepaid Card, and State Agency Disbursement Card products, where she was responsible for the strategy, marketing, and financial statement execution of these card programs. Doris holds a B.A. in Communications from the University of Southern California and an M.B.A from Wake Forest University Babcock School of Management.

Shannon Okine – Shannon supervises the Specialized Banking Unit at the Department of State Treasurer. Her team is responsible for cash flow management, monitoring the collateralization of public funds, as well as the set up and use of external State-owned accounts. She has been with the Department of State Treasurer for seven years and previously supervised the Disbursing Account Services unit, where she oversaw the State Treasurer's internal accounts, Positive Pay Program, and fraud cases. Shannon has 19 years of experience in branch banking, banking operations, and management. She received her degree in Economics from the University of North Carolina at Chapel Hill.

Luke Harris – Luke has been employed with the NC Office of the State Controller for over 15 years. For the past 11 years, he has held the position of Financial Specialist in the Statewide Accounting Division working with the Statewide Electronic Commerce Program. Luke holds a B.S. in Business Administration with a major in Accounting from Western Carolina University.

PCI Data Security Standards – Security Awareness Training

Shawn Ryan – Shawn is a Senior Security Engineer for Agio. He is a seasoned 15 year IT security professional in global industries, including telecommunications, data center, supply chain manufacturing, healthcare, pharmaceutical, education, and consulting industries. Shawn holds certifications from (ISC)2 including the CISSP and ISSMP. He attained the Certified in Risk and Information Systems Control (CRISC) certification from ISACA. He maintains certification as a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) in the Payment Card Industry Data Security Standard (PCI DSS) from the PCI Security Standards Council. Shawn specializes in security policy, compliance, incident response, and operations.

The Cost of Compromise

Special Agent Stanley Crowder – Stanley Crowder is a Special Agent (SA) with the United States Secret Service, currently assigned to the Raleigh, NC resident office. SA Crowder began his career in law enforcement as a Deputy Sheriff with the New Hanover County Sheriff's Office, Wilmington, NC from 1986 until 2000. In 2000, SA Crowder began his employment with the U.S. Secret Service in the Miami Field Office, where he investigated multiple credit card fraud causes. In 2002, SA Crowder became a member of the Electronic Crimes Special Agent Program, is a founding member of the Miami Electronic Crimes Task Force, and has received specialized training pertaining to the forensic analysis of electronic storage media. To date SA Crowder has received over 450 hours of training related to the forensic analysis of electronic storage media, to include Windows and Macintosh operating environments. SA Crowder has also served in the Criminal Investigative and Protective Services Divisions at Secret Service Headquarters in Washington, DC. SA Crowder is a graduate of the University of North Carolina at Wilmington with a Bachelor's Degree in Criminal Justice.

Panel Discussion – eCommerce in Government – "A Look at the Opportunities and Challenges"

Maurice Ferrell – Maurice is the Assistant Director, Center for Public Technology, at the UNC School of Government. His areas of expertise include networking, emerging technologies, virtual environments, technology planning, business intelligence, and network security. Before joining the School of Government in February 2009, Maurice served as chief information officer for the Institute for Advanced Learning and Research in Danville, Virginia. His efforts were recognized by the governor at the Commonwealth of Virginia Innovative Technology Symposium (COVITS) in 2004 for Technology Innovation in Higher Education. He also served as principal investigator for a three-year National Science Foundation grant that totaled $1 million, which focused on providing technology experiences for high school students. Previously, Maurice was the IT director for the Danville Public School System. Maurice earned an MBA from Liberty University, a bachelor's degree in business administration from Averett University, and an associate's degree in information technology from Danville Community College.

Carl Pickney – Carl has worked for the NC Department of Transportation since 1993 in the Information Technology Division. He has risen through the ranks starting as an Analyst/Application Developer and he currently holds the title of Information Security Manager – Advanced, where he oversees several Enterprise Applications in document and content management, software testing, and credit/debit card services. Previously, Carl worked for IBM as a Senior Associate Programmer. Carl received a B.S. degree in Computer Science and a Master of Science Degree in Computer Science from Southern University Agricultural & Mechanical College.

Dee Bowling – Dee is a CPA and works at the Director of Compliance Management for Financial Services at East Carolina University (ECU) and also serves as the project co-lead with the UNC FIT initiative for Student Accounts. During her 12 years with ECU, Dee also spent several years as the Director of Student Financial Services and as the Controller for the Medical and Health Sciences Foundation. She received her Bachelor of Science, Master of Business Administrations, and Master of Science in Accounting, all from ECU.

Rick Owens – Rick is Assistant Vice President of Information Technology and Administrative Services at Pitt Community College. He holds a BS in Computer Science and Master of Business Administration from East Carolina University and a Government Chief Information Officer Certification from the UNC School of Government.

Bill Greeves – Bill currently serves as the Chief Information Officer for Wake County, NC. Previously, he served as the CIO for Roanoke County, Virginia and the Director of Information Technology the City of Hampton, Virginia. He has been working in municipal government since 2000. In 2010, Government Technology magazine included him in their list of top 25 Doers, Dreamers and Drivers. In 2012, he was recognized by Pubic CIO magazine as the most social-media savvy CIO in government. Greeves is the co-author of the *Social Media in the Public Sector Field Guide: Designing and Implementing Strategies and Policies from Wiley Publishing*. Greeves holds a Master's degree from Old Dominion University and is a graduate of the University of Virginia's Senior Executive Institute.

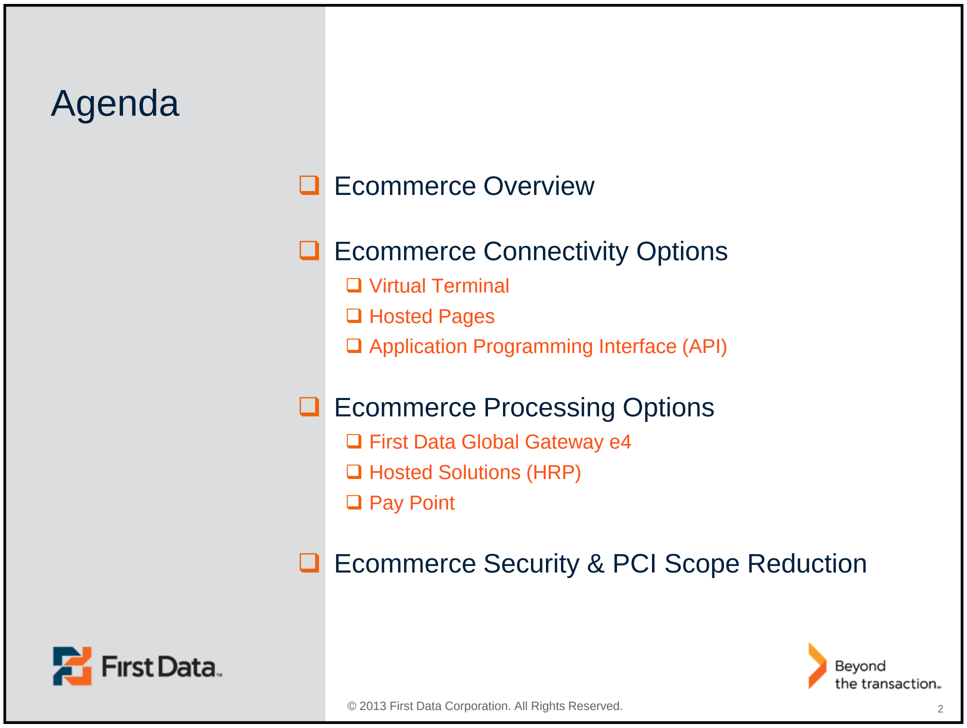
Emerging Trends in eCommerce

Rhonda Kirk, Stephanie Spencer & Alan Kelly
Product Solutions

April 30th 2014

First Data

Beyond the transaction.



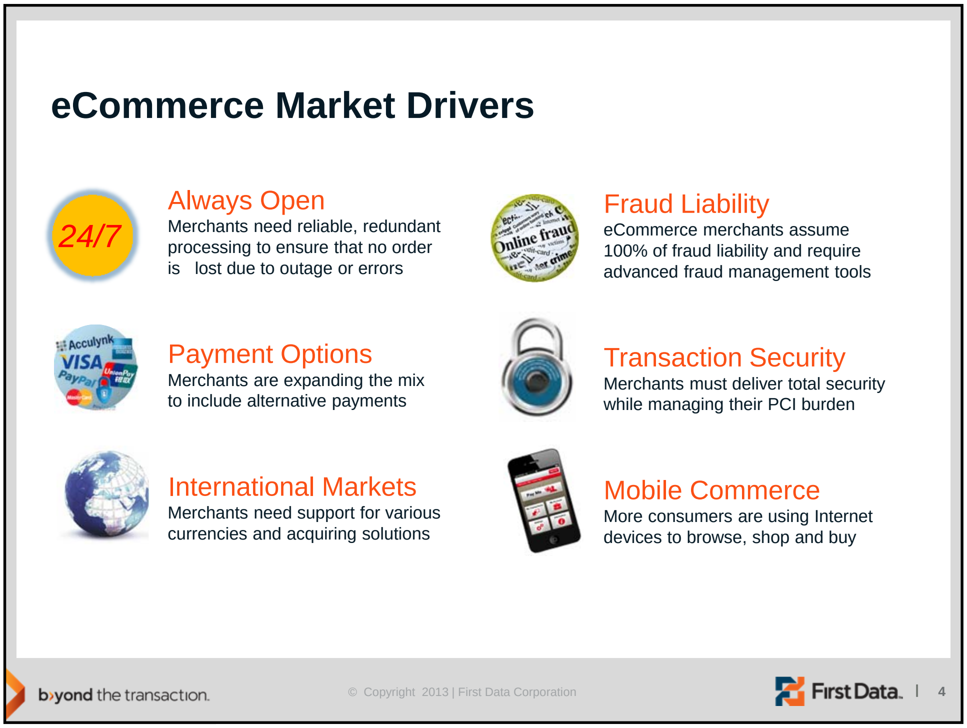
Agenda

- ❑ Ecommerce Overview
- ❑ Ecommerce Connectivity Options
  - ❑ Virtual Terminal
  - ❑ Hosted Pages
  - ❑ Application Programming Interface (API)
- ❑ Ecommerce Processing Options
  - ❑ First Data Global Gateway e4
  - ❑ Hosted Solutions (HRP)
  - ❑ Pay Point
- ❑ Ecommerce Security & PCI Scope Reduction

First Data

Beyond the transaction.

eCommerce Products



eCommerce Market Drivers

Always Open

Merchants need reliable, redundant processing to ensure that no order is   lost due to outage or errors

Fraud Liability

eCommerce merchants assume 100% of fraud liability and require advanced fraud management tools

Payment Options

Merchants are expanding the mix to include alternative payments

Transaction Security

Merchants must deliver total security while managing their PCI burden

International Markets

Merchants need support for various currencies and acquiring solutions

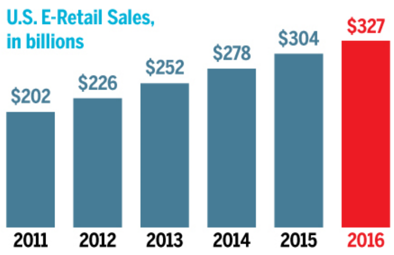
Mobile Commerce

More consumers are using Internet devices to browse, shop and buy

eCommerce Landscape & Trends

The number of web shoppers will continue to grow rapidly

1



U.S. E-commerce Sales: 2011-2016

Online consumers will increase their spending 62% by 2016, according to Forrester Inc.

Source: Forrester Inc.

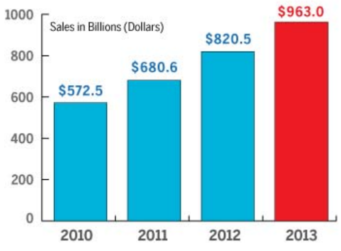
By 2016, it is estimated that …

- Online shoppers in the U.S. will spend $327B
- 192 million U.S. consumers will shop online[1]
- U.S. consumers will spend an average of $1,738 online[1]
- e-Retail will account for 9% of total retail sales[1]

[1] "U.S. Online Retail Forecast, 2011 to 2016" by Forrester Research Inc., February 2012

eCommerce Landscape & Trends (continued)

1



Global e-commerce sales are growing at more than 19% a year

Worldwide retail web sales will reach nearly $1 trillion by 2013, predicts Goldman Sachs. E-commerce is growing at 19.4%, the investment bank says.

Source: Goldman Sachs, Sales in billions of dollars.

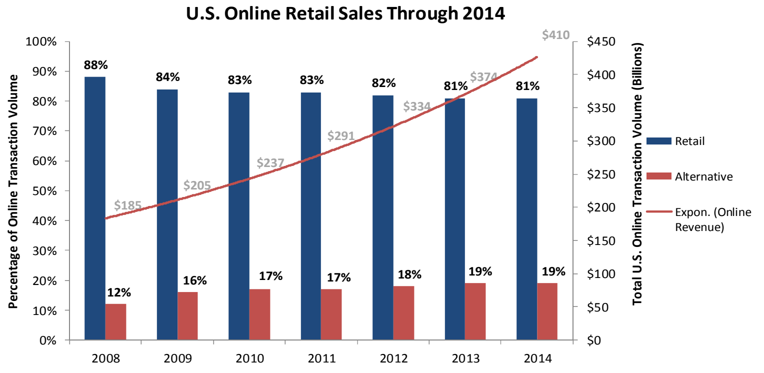
Globally…

- E-commerce revenue reached $680 billion worldwide in 2011, up 18.9% year-over-year[1]
- European online consumers this year will spend more than 305 billion euros, approximately $396.5 billion, up 20% from 254 billion euros ($330.2 billion) in 2011[2]

[1] J.P. Morgan: Global e-commerce Revenue to grow by 19% in 2011 to $680B', TechCrunch Newsroom , 2011
[2] eCommerce Europe

Alternative Payments

Online retail sales will continue steady growth with alternative payments representing a growing percentage of online transactions



Online Payments Forecast, Javelin Strategy & Research, February 2010

Alternative Payments

Popular choice for CNP merchants & shoppers due to security & convenience

- Enables merchants to conduct business globally
- No additional card data stored by merchant (PCI)
- Alternative providers assume or share fraud liability
  - Acculynk's PaySecure creates a PIN debit transaction - issuer takes liability
- Merchant transaction fees are often simplified or reduced (as opposed to interchange)

BillMe Later®

Google wallet

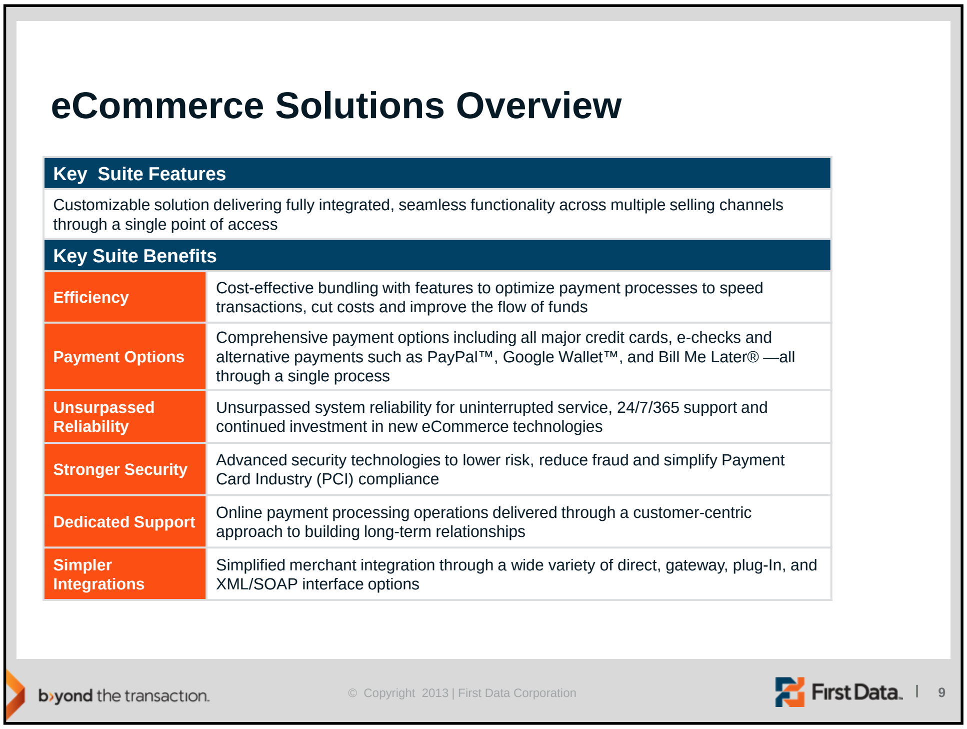
PaySecure

PayPal

TeleCheck®

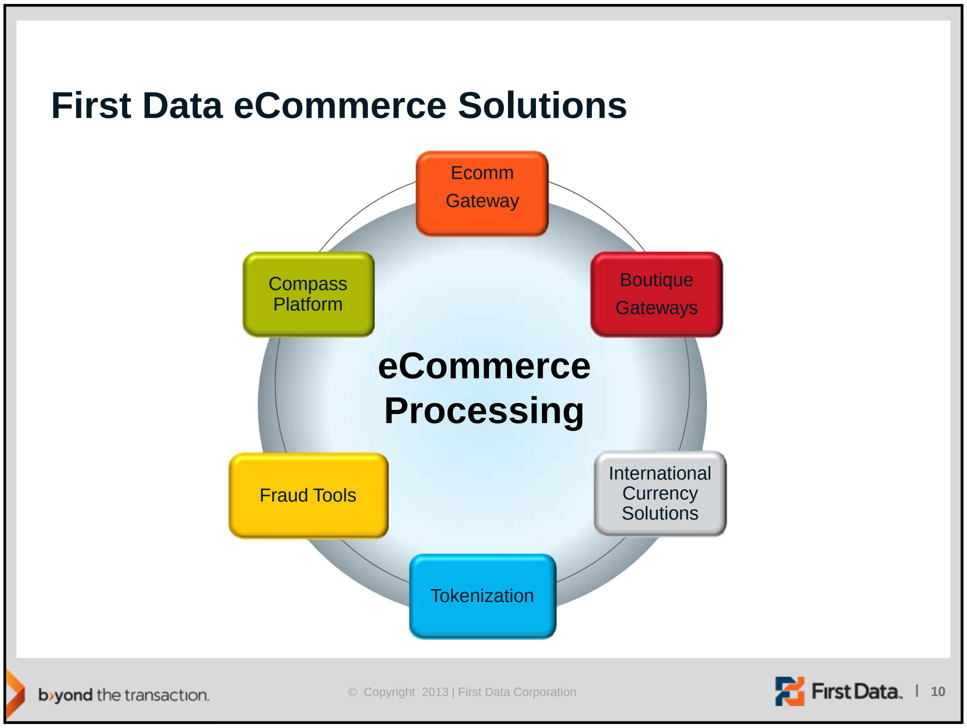
$110 Billion Projected eCommerce revenue from non-card payments in 2016, up from $64 billion in 2012

Source: "U.S. Alternative Payments Forecast, 2011 to 2016", Forrester Research Inc., May 2012

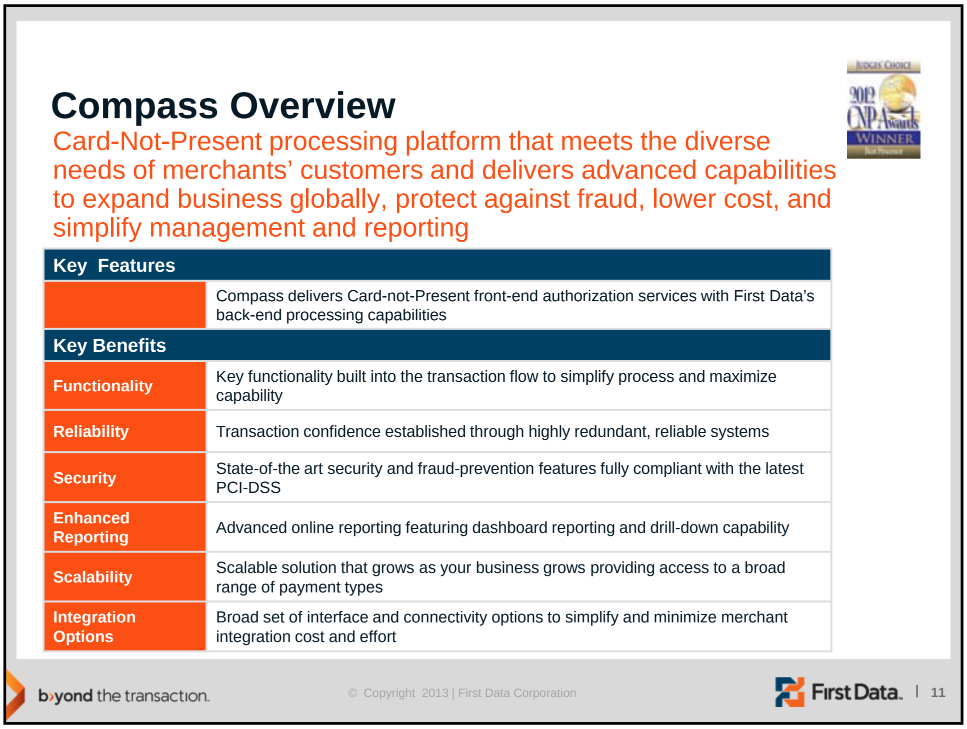


eCommerce Solutions Overview

Key Suite Features	
Customizable solution delivering fully integrated, seamless functionality across multiple selling channels through a single point of access	
Key Suite Benefits	
Efficiency	Cost-effective bundling with features to optimize payment processes to speed transactions, cut costs and improve the flow of funds
Payment Options	Comprehensive payment options including all major credit cards, e-checks and alternative payments such as PayPal™, Google Wallet™, and Bill Me Later® —all through a single process
Unsurpassed Reliability	Unsurpassed system reliability for uninterrupted service, 24/7/365 support and continued investment in new eCommerce technologies
Stronger Security	Advanced security technologies to lower risk, reduce fraud and simplify Payment Card Industry (PCI) compliance
Dedicated Support	Online payment processing operations delivered through a customer-centric approach to building long-term relationships
Simpler Integrations	Simplified merchant integration through a wide variety of direct, gateway, plug-In, and XML/SOAP interface options



First Data eCommerce Solutions

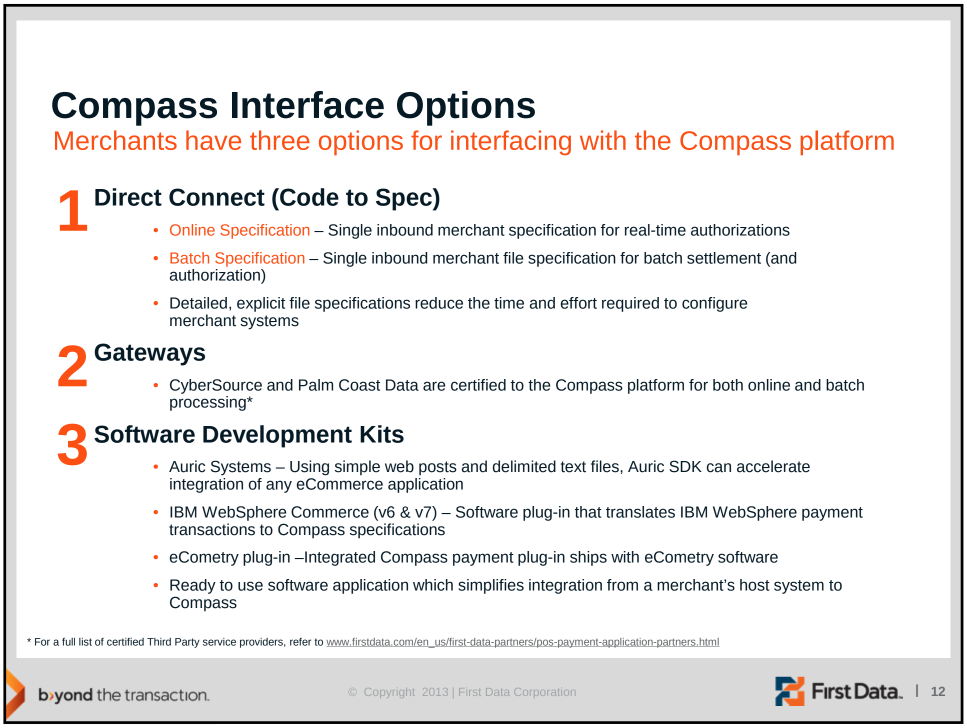


JUDGES' CHOICE
2012 CNP Awards
WINNER

Compass Overview

Card-Not-Present processing platform that meets the diverse needs of merchants' customers and delivers advanced capabilities to expand business globally, protect against fraud, lower cost, and simplify management and reporting

Key Features	
	Compass delivers Card-not-Present front-end authorization services with First Data's back-end processing capabilities
Key Benefits	
Functionality	Key functionality built into the transaction flow to simplify process and maximize capability
Reliability	Transaction confidence established through highly redundant, reliable systems
Security	State-of-the art security and fraud-prevention features fully compliant with the latest PCI-DSS
Enhanced Reporting	Advanced online reporting featuring dashboard reporting and drill-down capability
Scalability	Scalable solution that grows as your business grows providing access to a broad range of payment types
Integration Options	Broad set of interface and connectivity options to simplify and minimize merchant integration cost and effort



Compass Interface Options

Merchants have three options for interfacing with the Compass platform

1 Direct Connect (Code to Spec)

- Online Specification – Single inbound merchant specification for real-time authorizations
- Batch Specification – Single inbound merchant file specification for batch settlement (and authorization)
- Detailed, explicit file specifications reduce the time and effort required to configure merchant systems

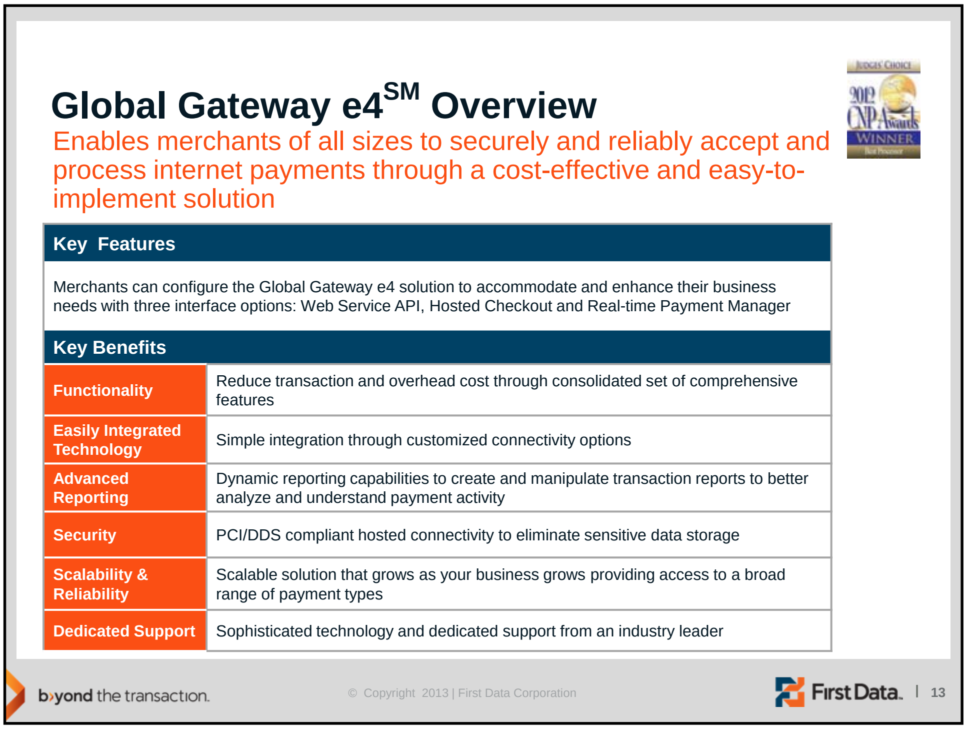
2 Gateways

- CyberSource and Palm Coast Data are certified to the Compass platform for both online and batch processing*

3 Software Development Kits

- Auric Systems – Using simple web posts and delimited text files, Auric SDK can accelerate integration of any eCommerce application
- IBM WebSphere Commerce (v6 & v7) – Software plug-in that translates IBM WebSphere payment transactions to Compass specifications
- eCometry plug-in –Integrated Compass payment plug-in ships with eCometry software
- Ready to use software application which simplifies integration from a merchant's host system to Compass

* For a full list of certified Third Party service providers, refer to www.firstdata.com/en_us/first-data-partners/pos-payment-application-partners.html

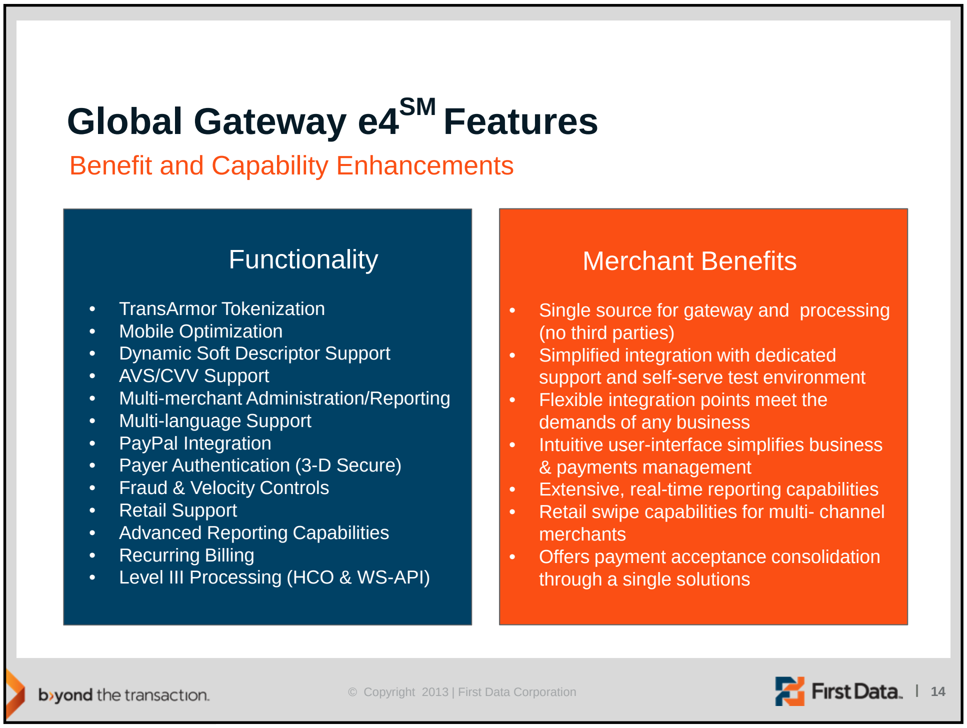


Global Gateway e4^{SM} Overview

Enables merchants of all sizes to securely and reliably accept and process internet payments through a cost-effective and easy-to-implement solution

JUDGES' CHOICE
2012 CNP Awards
WINNER
Best Processor

Key Features	
Merchants can configure the Global Gateway e4 solution to accommodate and enhance their business needs with three interface options: Web Service API, Hosted Checkout and Real-time Payment Manager	
Key Benefits	
Functionality	Reduce transaction and overhead cost through consolidated set of comprehensive features
Easily Integrated Technology	Simple integration through customized connectivity options
Advanced Reporting	Dynamic reporting capabilities to create and manipulate transaction reports to better analyze and understand payment activity
Security	PCI/DDS compliant hosted connectivity to eliminate sensitive data storage
Scalability & Reliability	Scalable solution that grows as your business grows providing access to a broad range of payment types
Dedicated Support	Sophisticated technology and dedicated support from an industry leader



Global Gateway e4^{SM} Features

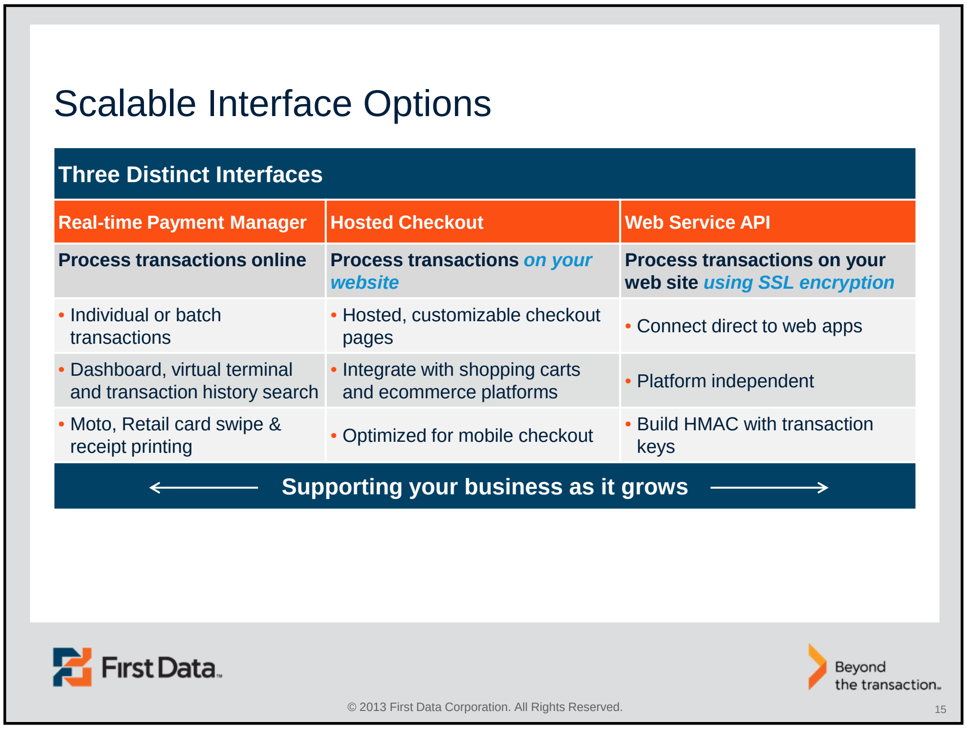
Benefit and Capability Enhancements

Functionality

- TransArmor Tokenization
- Mobile Optimization
- Dynamic Soft Descriptor Support
- AVS/CVV Support
- Multi-merchant Administration/Reporting
- Multi-language Support
- PayPal Integration
- Payer Authentication (3-D Secure)
- Fraud & Velocity Controls
- Retail Support
- Advanced Reporting Capabilities
- Recurring Billing
- Level III Processing (HCO & WS-API)

Merchant Benefits

- Single source for gateway and processing (no third parties)
- Simplified integration with dedicated support and self-serve test environment
- Flexible integration points meet the demands of any business
- Intuitive user-interface simplifies business & payments management
- Extensive, real-time reporting capabilities
- Retail swipe capabilities for multi- channel merchants
- Offers payment acceptance consolidation through a single solutions

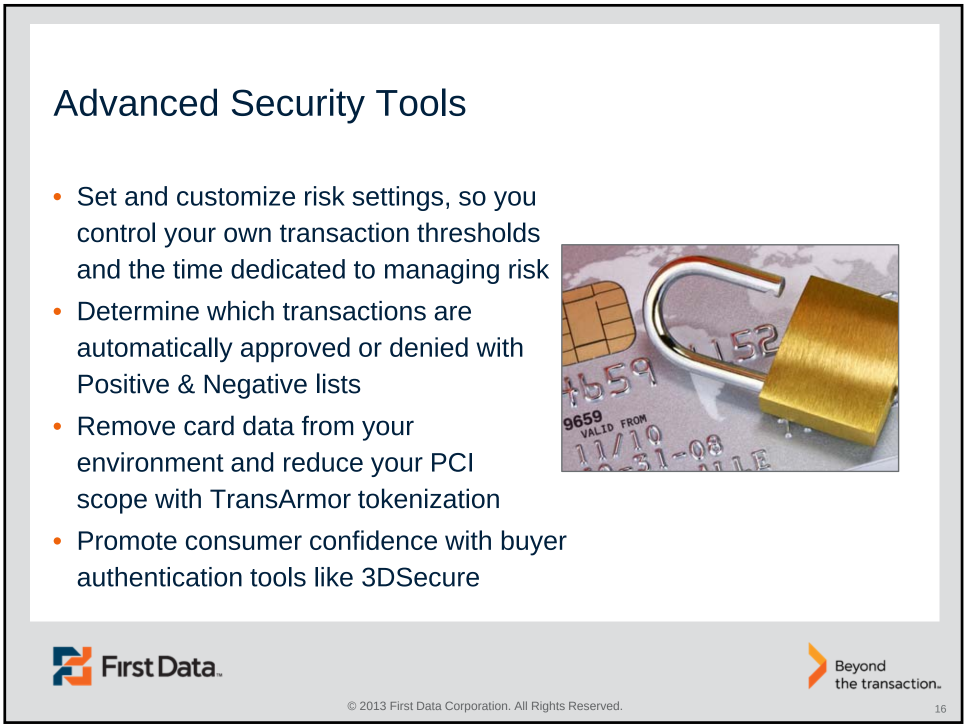


Scalable Interface Options

Three Distinct Interfaces		
Real-time Payment Manager	**Hosted Checkout**	**Web Service API**
Process transactions online	**Process transactions *on your website***	**Process transactions on your web site *using SSL encryption***
• Individual or batch transactions	• Hosted, customizable checkout pages	• Connect direct to web apps
• Dashboard, virtual terminal and transaction history search	• Integrate with shopping carts and ecommerce platforms	• Platform independent
• Moto, Retail card swipe & receipt printing	• Optimized for mobile checkout	• Build HMAC with transaction keys
← **Supporting your business as it grows** →		

First Data.

Beyond the transaction.

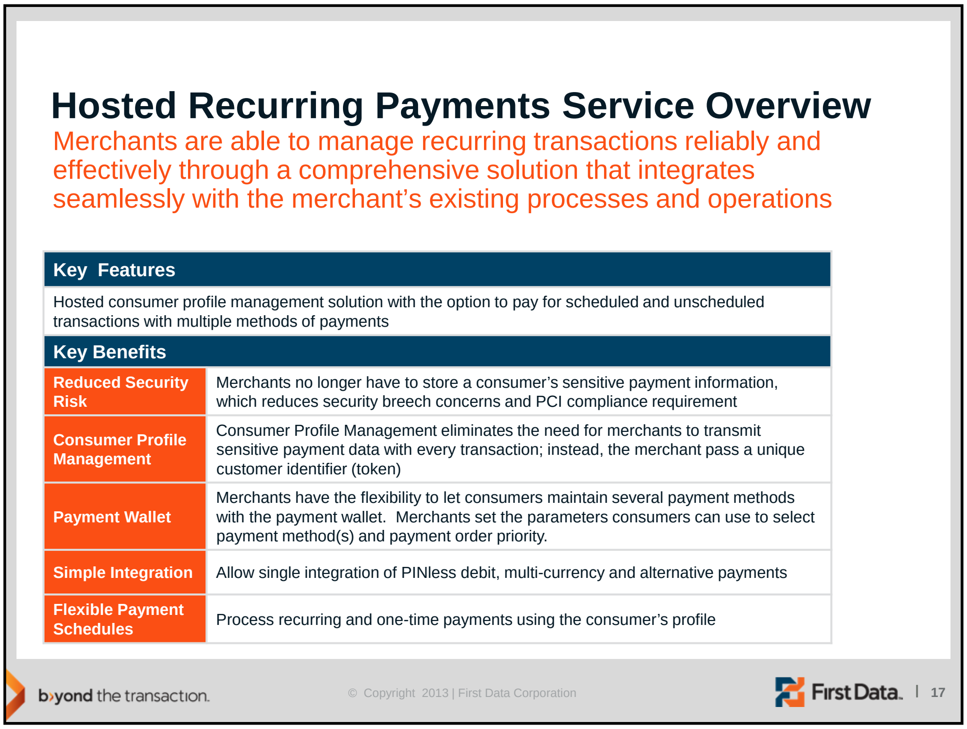


Advanced Security Tools

- Set and customize risk settings, so you control your own transaction thresholds and the time dedicated to managing risk
- Determine which transactions are automatically approved or denied with Positive & Negative lists
- Remove card data from your environment and reduce your PCI scope with TransArmor tokenization
- Promote consumer confidence with buyer authentication tools like 3DSecure

First Data.

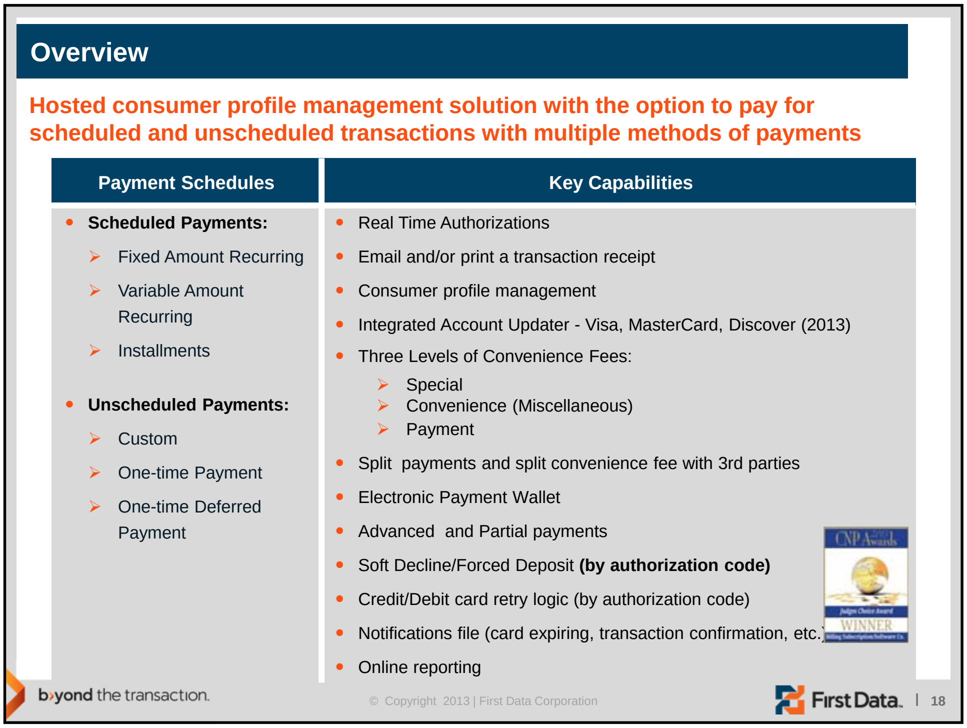
Beyond the transaction.



Hosted Recurring Payments Service Overview

Merchants are able to manage recurring transactions reliably and effectively through a comprehensive solution that integrates seamlessly with the merchant’s existing processes and operations

Key Features	
Hosted consumer profile management solution with the option to pay for scheduled and unscheduled transactions with multiple methods of payments	
Key Benefits	
Reduced Security Risk	Merchants no longer have to store a consumer’s sensitive payment information, which reduces security breech concerns and PCI compliance requirement
Consumer Profile Management	Consumer Profile Management eliminates the need for merchants to transmit sensitive payment data with every transaction; instead, the merchant pass a unique customer identifier (token)
Payment Wallet	Merchants have the flexibility to let consumers maintain several payment methods with the payment wallet. Merchants set the parameters consumers can use to select payment method(s) and payment order priority.
Simple Integration	Allow single integration of PINless debit, multi-currency and alternative payments
Flexible Payment Schedules	Process recurring and one-time payments using the consumer’s profile



Overview

Hosted consumer profile management solution with the option to pay for scheduled and unscheduled transactions with multiple methods of payments

Payment Schedules

- **Scheduled Payments:**
  - Fixed Amount Recurring
  - Variable Amount Recurring
  - Installments
- **Unscheduled Payments:**
  - Custom
  - One-time Payment
  - One-time Deferred Payment

Key Capabilities

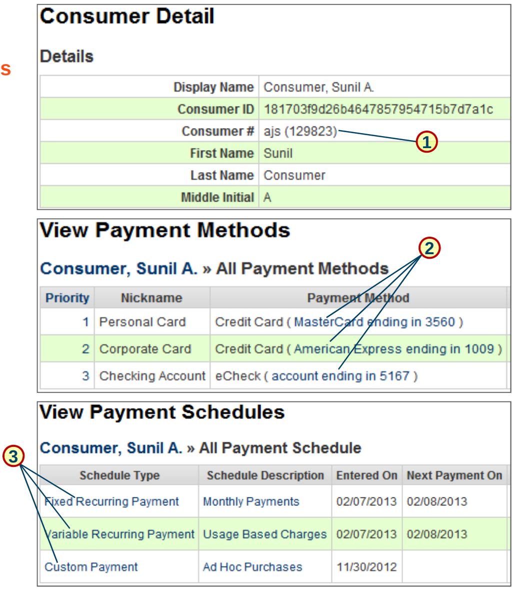
- Real Time Authorizations
- Email and/or print a transaction receipt
- Consumer profile management
- Integrated Account Updater - Visa, MasterCard, Discover (2013)
- Three Levels of Convenience Fees:
  - Special
  - Convenience (Miscellaneous)
  - Payment
- Split payments and split convenience fee with 3rd parties
- Electronic Payment Wallet
- Advanced and Partial payments
- Soft Decline/Forced Deposit **(by authorization code)**
- Credit/Debit card retry logic (by authorization code)
- Notifications file (card expiring, transaction confirmation, etc.)
- Online reporting

Consumer Profile Management

Allows merchants to securely store, retrieve, edit, and use consumer profile for scheduled and unscheduled payments

Benefits of Consumer Profile Manager

1. Reduces scope of PCI compliance
2. Uses a unique identifier to represent consumer data for future transactions
3. Stores payment credentials eliminating need to enter or pass sensitive data with each transaction
4. Eliminates need for merchant to physically store sensitive consumer payment data
5. Provides ability to have several payment schedules in each consumer profile with dedicated payment methods per schedule



Consumer Detail

Details

Display Name	Consumer, Sunil A.
Consumer ID	181703f9d26b4647857954715b7d7a1c
Consumer #	ajs (129823)
First Name	Sunil
Last Name	Consumer
Middle Initial	A

View Payment Methods

Consumer, Sunil A. » All Payment Methods

Priority	Nickname	Payment Method
1	Personal Card	Credit Card (MasterCard ending in 3560)
2	Corporate Card	Credit Card (American Express ending in 1009)
3	Checking Account	eCheck (account ending in 5167)

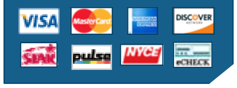
View Payment Schedules

Consumer, Sunil A. » All Payment Schedule

Schedule Type	Schedule Description	Entered On	Next Payment On
Fixed Recurring Payment	Monthly Payments	02/07/2013	02/08/2013
Variable Recurring Payment	Usage Based Charges	02/07/2013	02/08/2013
Custom Payment	Ad Hoc Purchases	11/30/2012	

PayPoint® Payment Gateway Capabilities

Multiple Payment Mediums



Multiple Payment Channels
Web, IVR, Recurring, Kiosk, POS, Face-to-Face

Convenience Fee Management

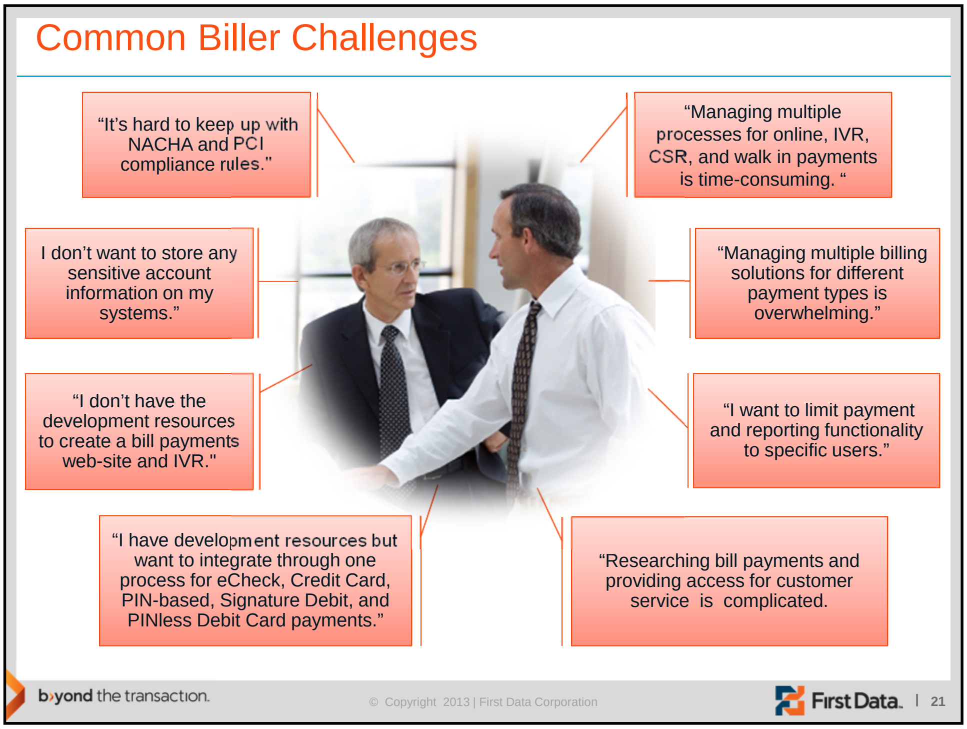
Advanced Duplicate Payment Detection

Enrollment & Recurring Payment Management
Stored Account Data & Flexible Recurrence Patterns

Fraud and Identity Verification Services
AVS, CVV2, TeleCheck® Processing

Full ACH Service
Returns, Refunds, eCheck Warranty, NOC

Flexible Cross Reference to Biller Transaction



Common Biller Challenges

"It's hard to keep up with NACHA and PCI compliance rules."

"Managing multiple processes for online, IVR, CSR, and walk in payments is time-consuming. "

I don't want to store any sensitive account information on my systems."

"Managing multiple billing solutions for different payment types is overwhelming."

"I don't have the development resources to create a bill payments web-site and IVR."

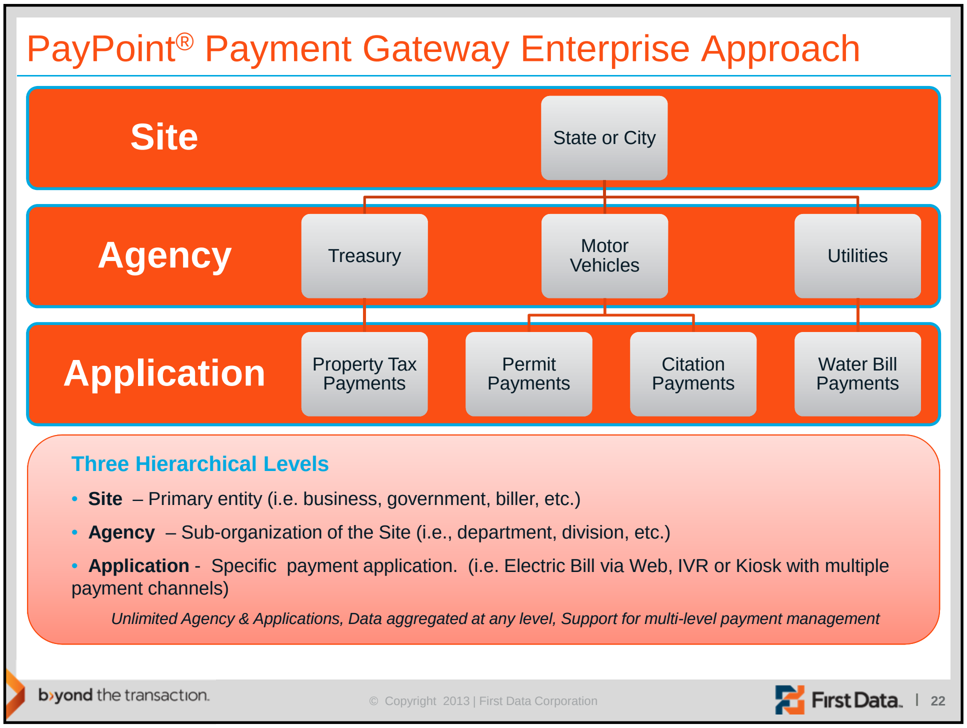
"I want to limit payment and reporting functionality to specific users."

"I have development resources but want to integrate through one process for eCheck, Credit Card, PIN-based, Signature Debit, and PINless Debit Card payments."

"Researching bill payments and providing access for customer service is complicated.

b›yond the transaction.

First Data. | 21



PayPoint® Payment Gateway Enterprise Approach

Three Hierarchical Levels

- **Site** – Primary entity (i.e. business, government, biller, etc.)
- **Agency** – Sub-organization of the Site (i.e., department, division, etc.)
- **Application** - Specific payment application. (i.e. Electric Bill via Web, IVR or Kiosk with multiple payment channels)

Unlimited Agency & Applications, Data aggregated at any level, Support for multi-level payment management

b›yond the transaction.

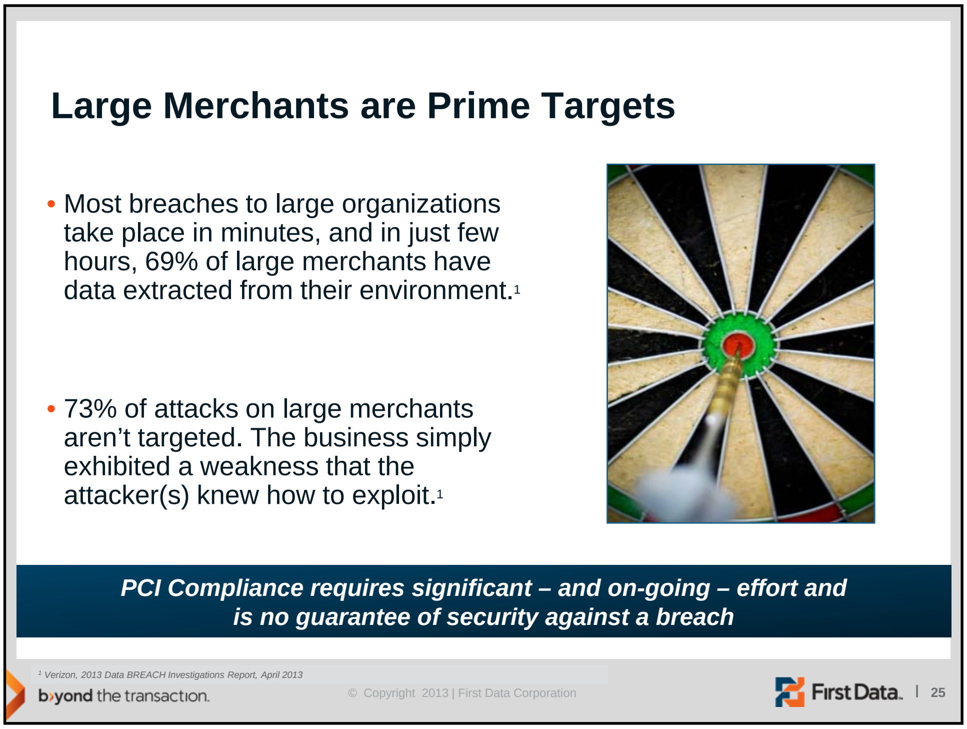
First Data. | 22

Tokenization & Encryption

Data Breaches are on the Rise

- In 2012, payment card information was again involved in more (61%) breaches than any other data type[1]
- This represents an increase of 13% from 2011, when payment card data represented 48% of the data compromised during a breach[1]

[1] Verizon, 2013 Data BREACH Investigations Report, April 2013

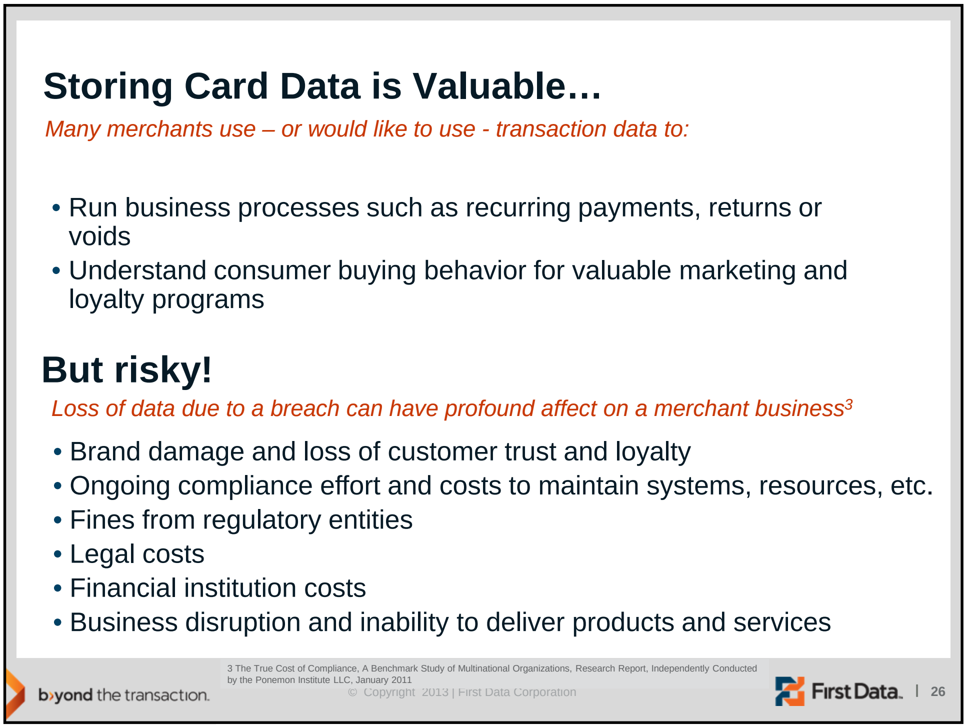


Large Merchants are Prime Targets

- Most breaches to large organizations take place in minutes, and in just few hours, 69% of large merchants have data extracted from their environment.[1]
- 73% of attacks on large merchants aren't targeted. The business simply exhibited a weakness that the attacker(s) knew how to exploit.[1]

PCI Compliance requires significant – and on-going – effort and is no guarantee of security against a breach

[1] *Verizon, 2013 Data BREACH Investigations Report, April 2013*



Storing Card Data is Valuable…

Many merchants use – or would like to use - transaction data to:

- Run business processes such as recurring payments, returns or voids
- Understand consumer buying behavior for valuable marketing and loyalty programs

But risky!

Loss of data due to a breach can have profound affect on a merchant business[3]

- Brand damage and loss of customer trust and loyalty
- Ongoing compliance effort and costs to maintain systems, resources, etc.
- Fines from regulatory entities
- Legal costs
- Financial institution costs
- Business disruption and inability to deliver products and services

[3] The True Cost of Compliance, A Benchmark Study of Multinational Organizations, Research Report, Independently Conducted by the Ponemon Institute LLC, January 2011

The Costs of a Data Breach are Staggering

- Total average cost per breach: $5.5M
  - Average number of breached records: 28,349
  - Average cost per breached record – overall: $194
- Average annual *additional* customer churn - or loss due to a data breach - was 3.2%, or an additional $3.0M*
- 78% of consumers said they would stop shopping at a store if they believed the store had experienced a card data compromise.

Michaels Breach Bigger than Reported

May 12, 2011 | Biometric Signature identity Theft Security News

Credit Card Breach May Cost Sony $24 Billion

arah LeBoeuf | 27 Apr 2011 3:06 pm

iled under: sarah leboeuf, credit card, hacker, playstation network, psn dowr

inancial analysts have estimated that Sony's possible oss of account information may cost the company illions of dollars in damages.

ony is not certain that personal credit card information vas stolen but admitted such theft was a possibility, but

78% of companies surveyed had already experienced a breach in prior years

* 2011 Cost of a Data Breach Study: United States" published March 2012

Reduce the Risk of Payment Card Data Breach

- Support a multi-layered approach to payment card protection
- Reduce the number of places where card data exists
  - Point-of Sale systems
  - CRM systems
  - MIS databases / reports
- Transfer burden of storing payment card data from merchant to processor
- Reduce the Card Data Environment (CDE) and therefore PCI compliance efforts

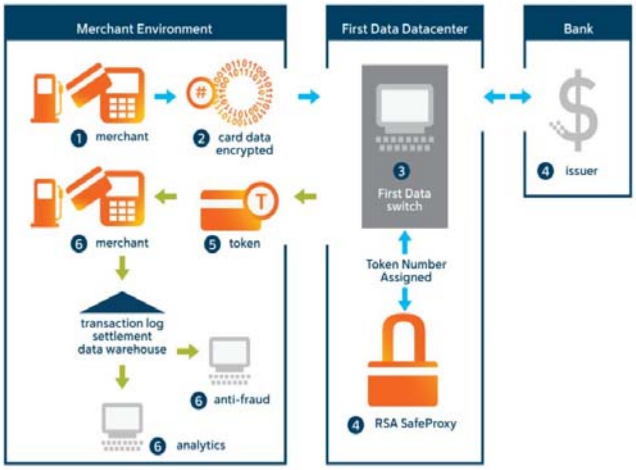
The First Data® TransArmor® Solution

What is the TransArmor Solution?

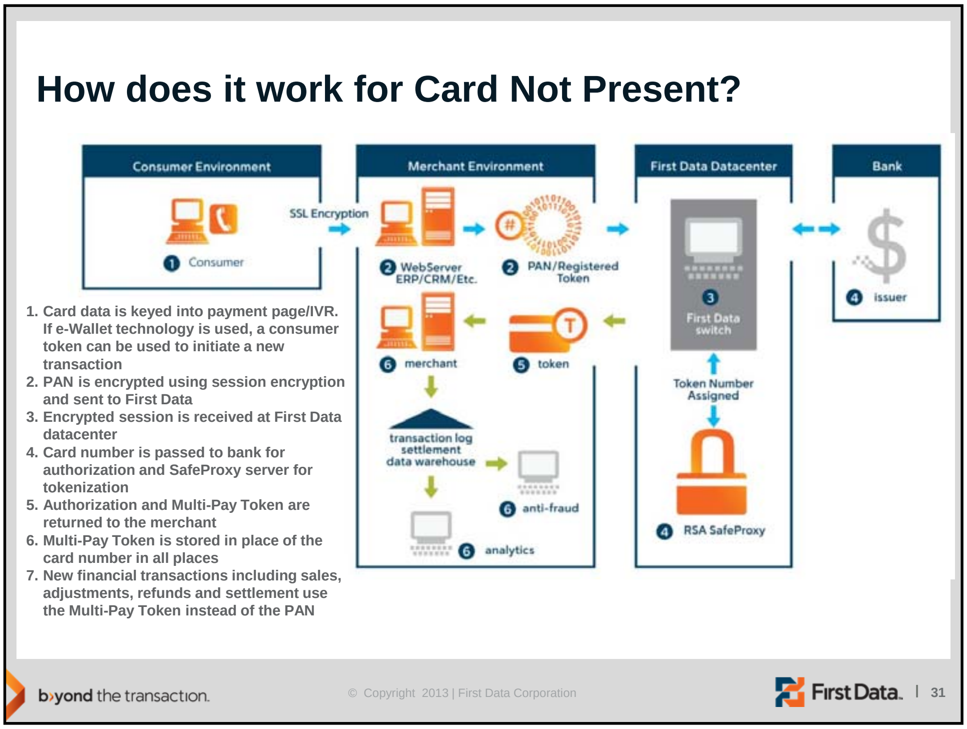
- A combination of encryption and tokenization technologies
  - Encryption protects data on the front end
  - Tokenization removes card data from the merchant environment post-authorization

	Card Present	Card Not Present
Hardware or software-based encryption secures the transaction	✓	✓
TransArmor Tokens remove card data from the merchant environment	✓	✓
Multi-Pay Tokens support recurring payments or reporting that drives business decisions and loyalty programs	✓	✓

How does it work for Card Present?

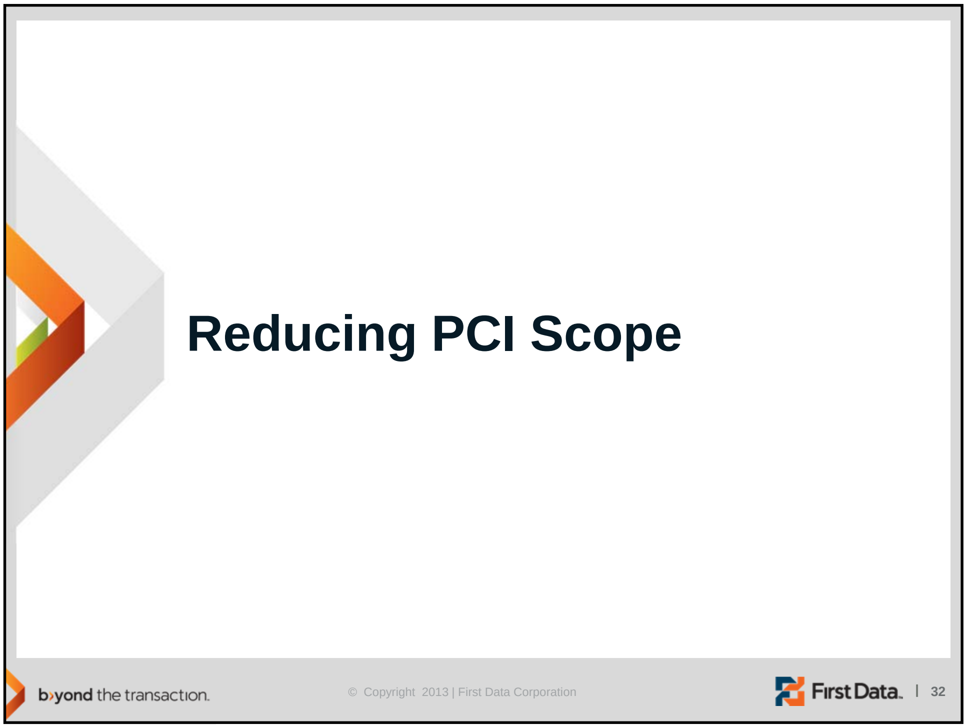


1. Consumer presents card to merchant
2. Card Data is encrypted and transmitted to First Data front-end
3. First Data front-end decrypts the data payload
4. Card data is sent to issuing bank for authorization and, in parallel, tokenized
5. Token is paired with authorization response and sent back to the merchant
6. Merchant stores token instead of card data in their environment and uses token for all subsequent business processes

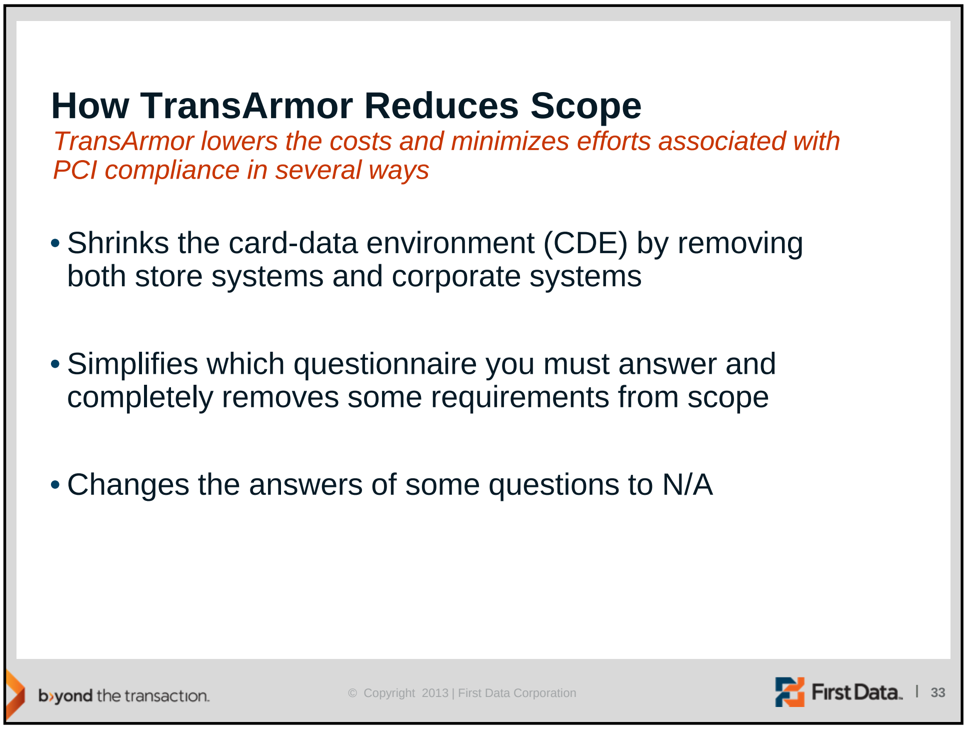


How does it work for Card Not Present?

1. Card data is keyed into payment page/IVR. If e-Wallet technology is used, a consumer token can be used to initiate a new transaction
2. PAN is encrypted using session encryption and sent to First Data
3. Encrypted session is received at First Data datacenter
4. Card number is passed to bank for authorization and SafeProxy server for tokenization
5. Authorization and Multi-Pay Token are returned to the merchant
6. Multi-Pay Token is stored in place of the card number in all places
7. New financial transactions including sales, adjustments, refunds and settlement use the Multi-Pay Token instead of the PAN



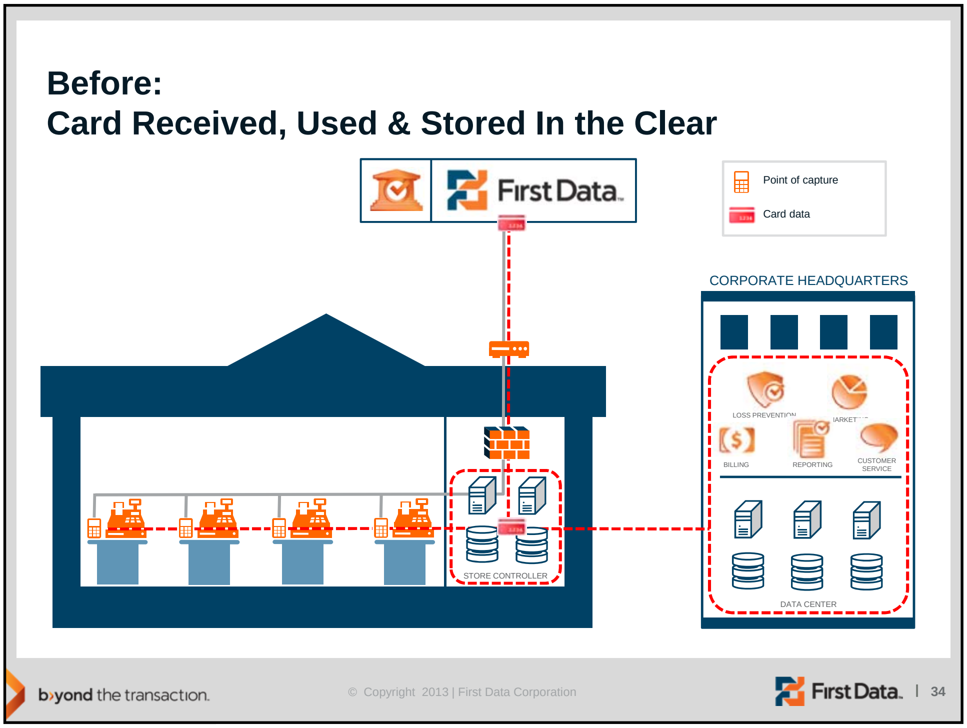
Reducing PCI Scope



How TransArmor Reduces Scope

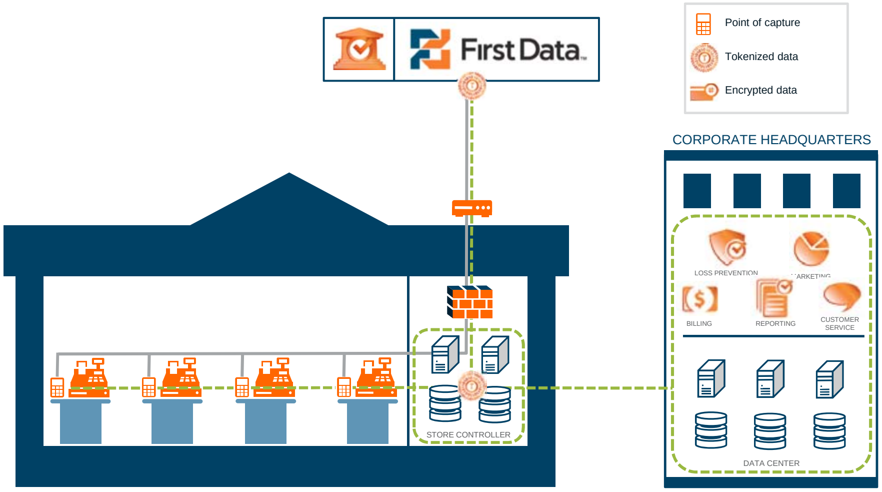
TransArmor lowers the costs and minimizes efforts associated with PCI compliance in several ways

- Shrinks the card-data environment (CDE) by removing both store systems and corporate systems
- Simplifies which questionnaire you must answer and completely removes some requirements from scope
- Changes the answers of some questions to N/A

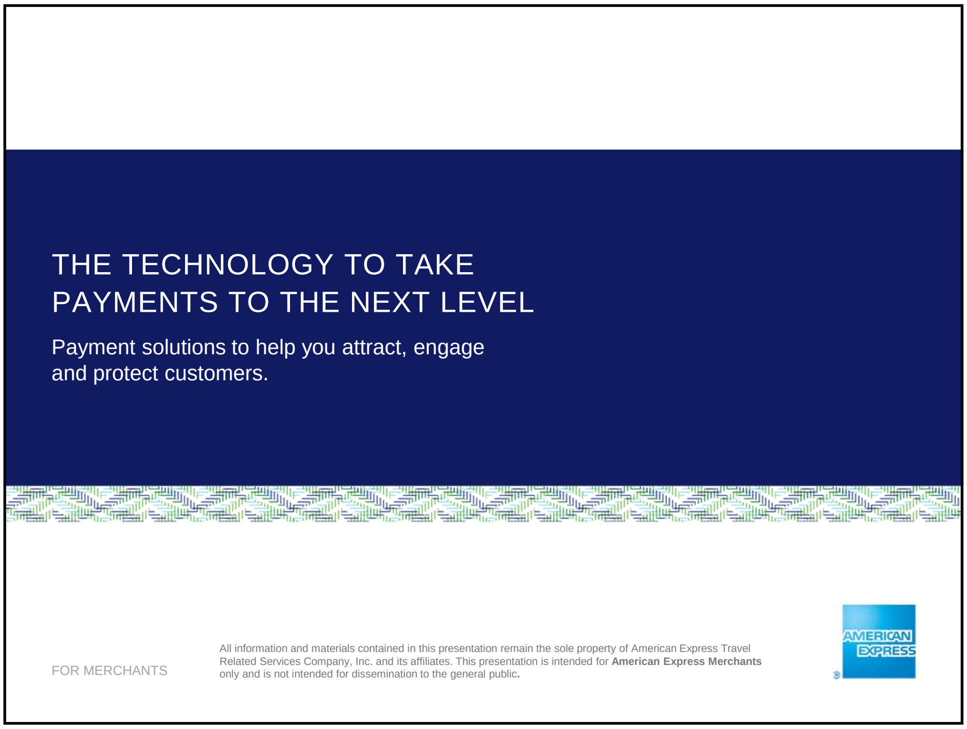


Before:
Card Received, Used & Stored In the Clear

After:
Tokenized Data Protects Entire CDE



Thank You!



THE TECHNOLOGY TO TAKE PAYMENTS TO THE NEXT LEVEL

Payment solutions to help you attract, engage and protect customers.

FOR MERCHANTS

Topics

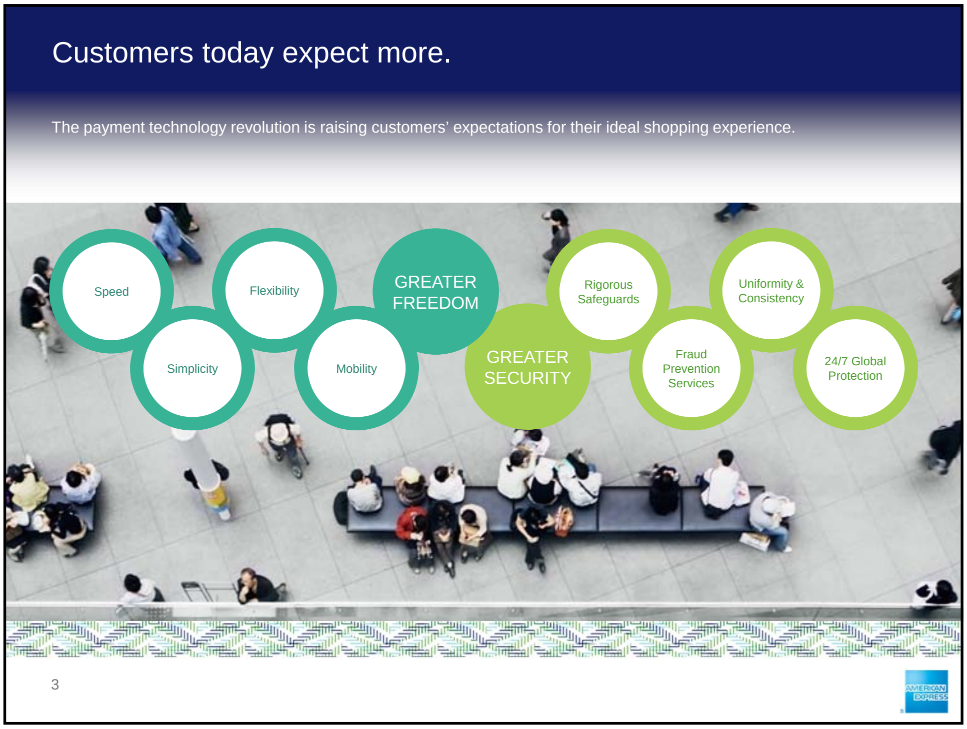
1 Introduction

2 EMV Chip Cards and Terminals

3 Contactless

4 Mobile Near-Field Communications (NFC)

2



Customers today expect more.

The payment technology revolution is raising customers' expectations for their ideal shopping experience.

Speed

Simplicity

Flexibility

Mobility

GREATER FREEDOM

GREATER SECURITY

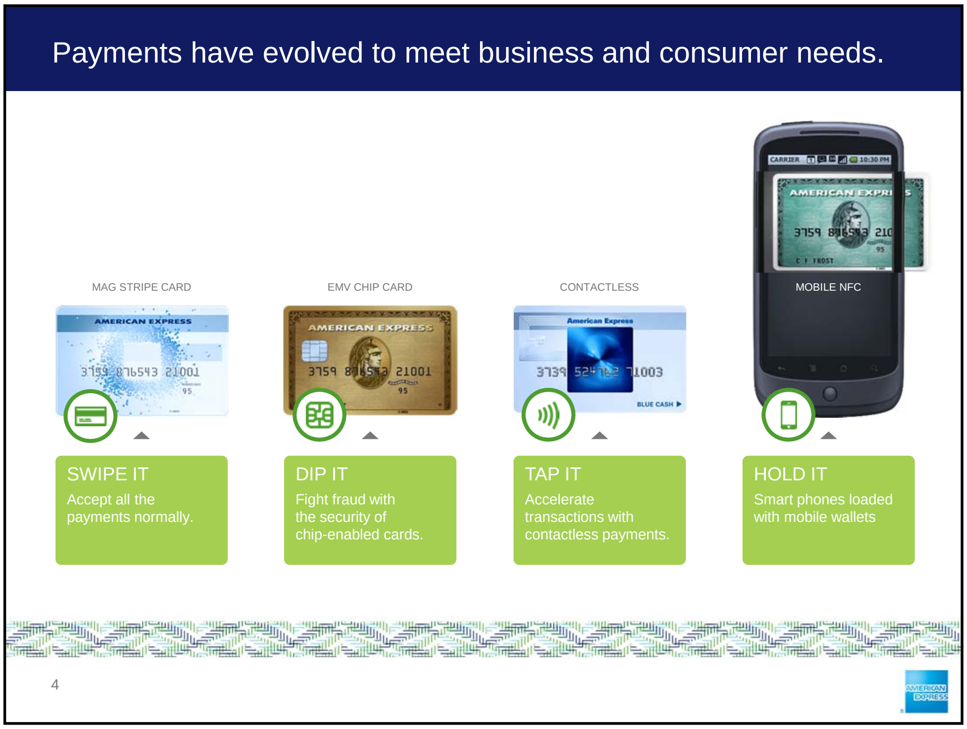
Rigorous Safeguards

Fraud Prevention Services

Uniformity & Consistency

24/7 Global Protection

3



Payments have evolved to meet business and consumer needs.

MAG STRIPE CARD

EMV CHIP CARD

CONTACTLESS

MOBILE NFC

SWIPE IT
Accept all the payments normally.

DIP IT
Fight fraud with the security of chip-enabled cards.

TAP IT
Accelerate transactions with contactless payments.

HOLD IT
Smart phones loaded with mobile wallets

4

EMV CHIP CARDS

Establish a secure payment foundation to advance business.

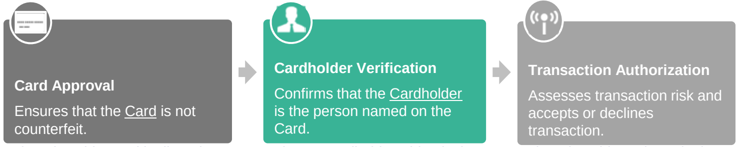
AMERICAN EXPRESS

What is EMV?

EMV IS A SET OF STANDARDS IN THE PAYMENTS INDUSTRY FOR CHIP-BASED TRANSACTION PROCESSING IN WHICH THE CARD HAS AN EMBEDDED MICROPROCESSOR CHIP THAT EXCHANGES DATA WITH THE TERMINAL, DELIVERING A MORE SECURE TRANSACTION.*

- What EMV means for cards:
  - Cards can be both Chip & Signature, requiring a signature, and Chip & PIN, requiring a PIN, to authorize the transaction.
  - Can be used in a contact and contactless payment environment.
- What EMV means for terminals:
  - Only relevant for card-present transactions.
  - Require terminals that can process EMV chip-based contact, contactless and mobile NFC, as well as magnetic stripe transactions.

Example: Contact EMV "Smart Cards"



Card Approval

Ensures that the Card is not counterfeit.

When the Chip Card is dipped into the terminal, the embedded microchip exchanges Card data with the terminal to verify the Card is genuine.

Cardholder Verification

Confirms that the Cardholder is the person named on the Card.

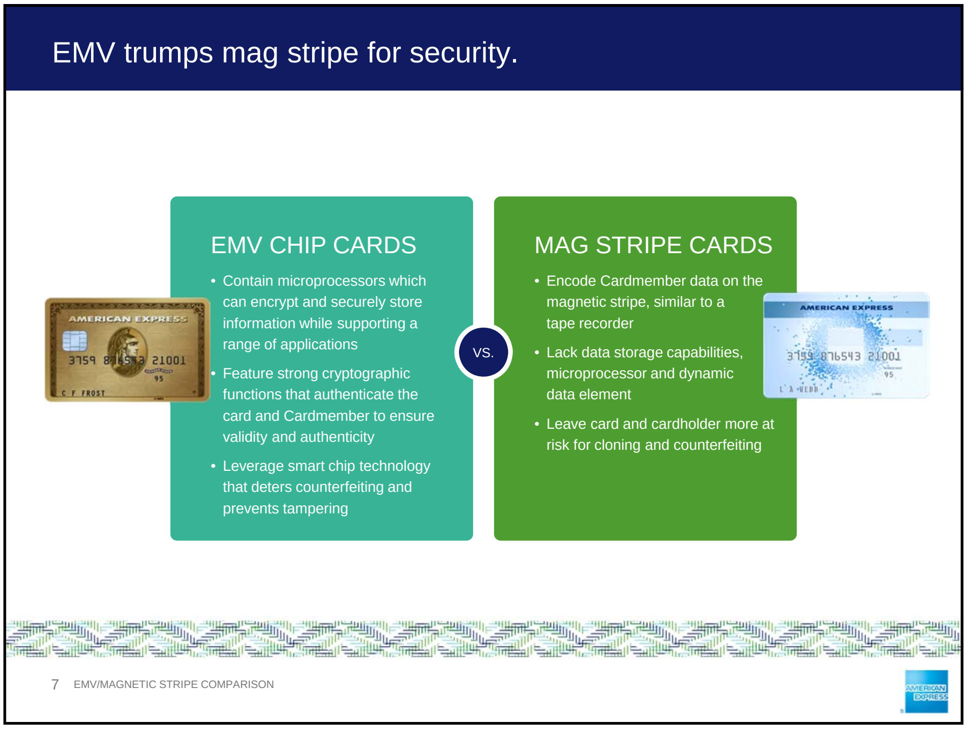
When a Cardholder's identity is verified with PIN or Signature, the Card then securely passes information to the issuer to perform additional authentication.

Transaction Authorization

Assesses transaction risk and accepts or declines transaction.

The microchip and terminal interact to assess the transaction details, providing issuers and Merchants better ability to control risk on every purchase.

*Europay, MasterCard and Visa formed EMVCo to develop and maintain the open specifications for global interoperability between chip cards and terminals for credit and debit payment irrespective of card brand, terminal, etc. American Express and JCB joined the company at a later date.



EMV trumps mag stripe for security.

EMV CHIP CARDS

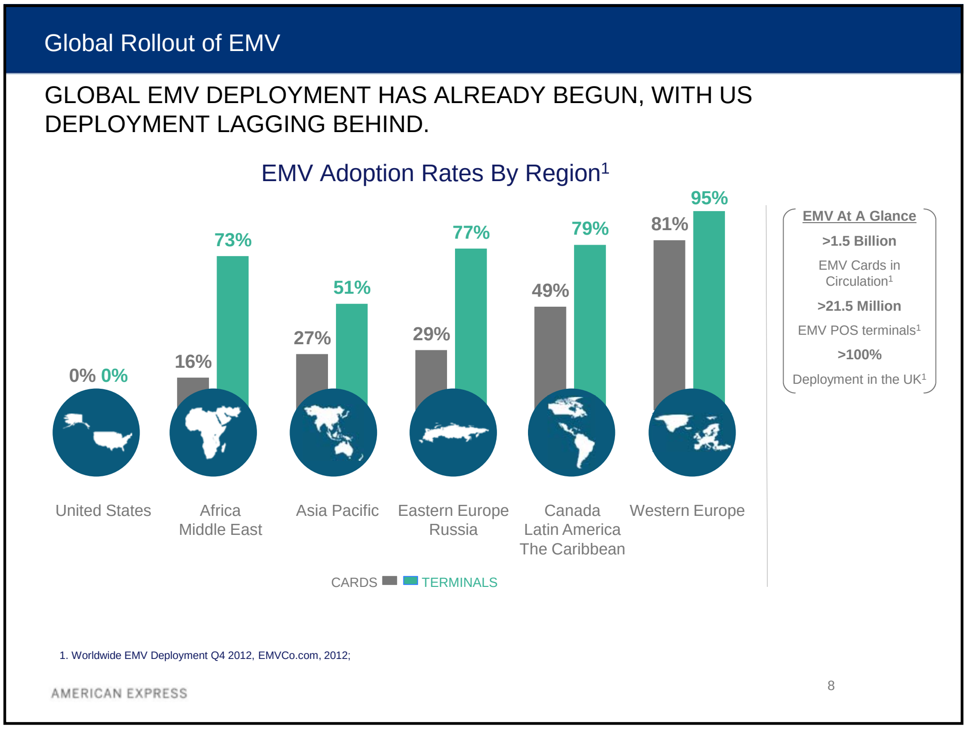
- Contain microprocessors which can encrypt and securely store information while supporting a range of applications
- Feature strong cryptographic functions that authenticate the card and Cardmember to ensure validity and authenticity
- Leverage smart chip technology that deters counterfeiting and prevents tampering

VS.

MAG STRIPE CARDS

- Encode Cardmember data on the magnetic stripe, similar to a tape recorder
- Lack data storage capabilities, microprocessor and dynamic data element
- Leave card and cardholder more at risk for cloning and counterfeiting

7 EMV/MAGNETIC STRIPE COMPARISON



Global Rollout of EMV

GLOBAL EMV DEPLOYMENT HAS ALREADY BEGUN, WITH US DEPLOYMENT LAGGING BEHIND.

EMV Adoption Rates By Region[1]

EMV At A Glance

>1.5 Billion

EMV Cards in Circulation[1]

>21.5 Million

EMV POS terminals[1]

>100%

Deployment in the UK[1]

[1] Worldwide EMV Deployment Q4 2012, EMVCo.com, 2012;

AMERICAN EXPRESS

8

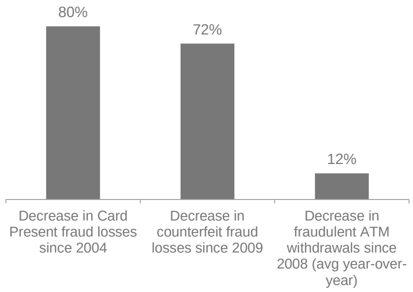
Global Results of Converting to EMV

SINCE ROLLING OUT EMV, GLOBAL MARKETS HAVE SEEN A REDUCTION IN MANY TYPES OF CREDIT CARD FRAUD.

With EMV – the UK

The EMV standard was rolled out in the UK as a mandatory requirement by 2005. Reductions in fraud were realized across all payment venues.

Decreases in various types of fraud in the UK since implementing EMV[1]



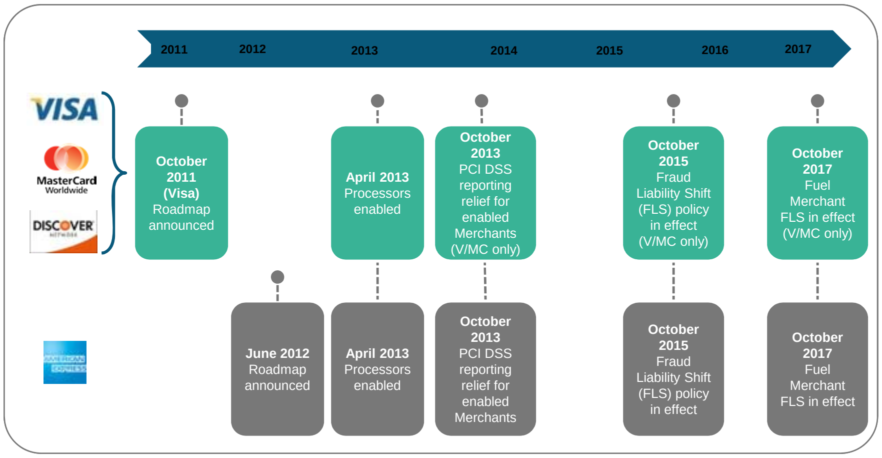
1. Fraud Facts Action UK 2012, 2. Federal Reserve Bank of Atlanta, Chip-and-PIN: Success and Challenges in Reducing Fraud, 2012,

Without EMV – the US

In the absence of EMV, the US has seen credit and charge card fraud levels increase over the last decade.

AMERICAN EXPRESS

US Rollout – Industry-Wide Roadmap



October 2011 (Visa) Roadmap announced

April 2013 Processors enabled

October 2013 PCI DSS reporting relief for enabled Merchants (V/MC only)

October 2015 Fraud Liability Shift (FLS) policy in effect (V/MC only)

October 2017 Fuel Merchant FLS in effect (V/MC only)

June 2012 Roadmap announced

April 2013 Processors enabled

October 2013 PCI DSS reporting relief for enabled Merchants

October 2015 Fraud Liability Shift (FLS) policy in effect

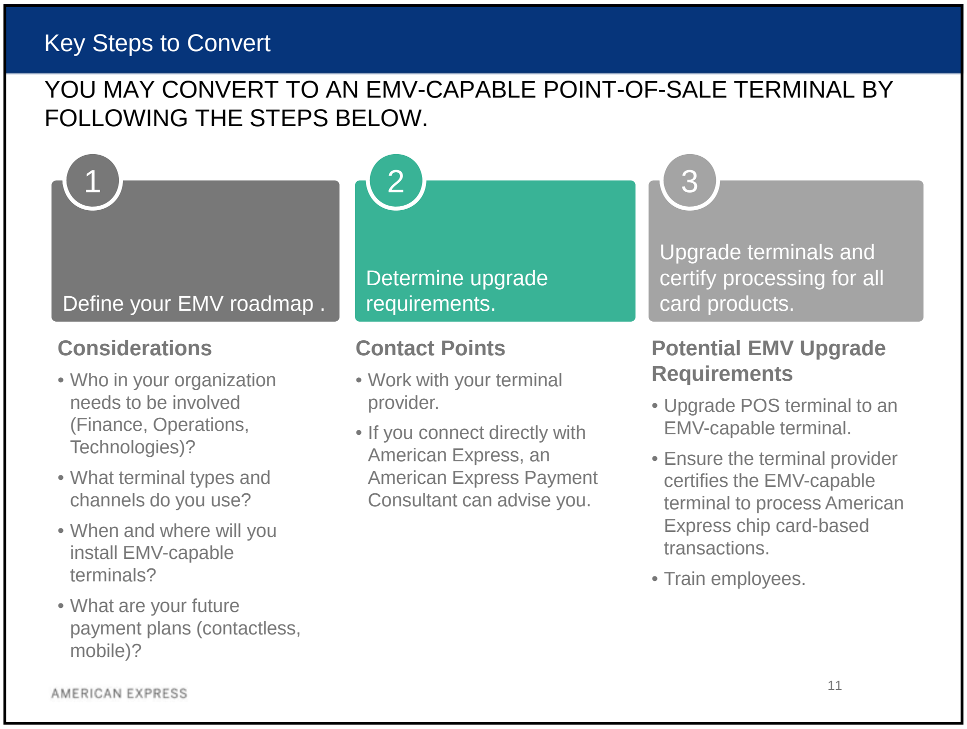
October 2017 Fuel Merchant FLS in effect

Card Migration Status

- American Express proprietary issuers began migrating portfolios to EMV Cards in late 2012.
- Migration will continue across all proprietary portfolios through 2015.

10

AMERICAN EXPRESS



Key Steps to Convert

YOU MAY CONVERT TO AN EMV-CAPABLE POINT-OF-SALE TERMINAL BY FOLLOWING THE STEPS BELOW.

1 Define your EMV roadmap .

2 Determine upgrade requirements.

3 Upgrade terminals and certify processing for all card products.

Considerations

- Who in your organization needs to be involved (Finance, Operations, Technologies)?
- What terminal types and channels do you use?
- When and where will you install EMV-capable terminals?
- What are your future payment plans (contactless, mobile)?

Contact Points

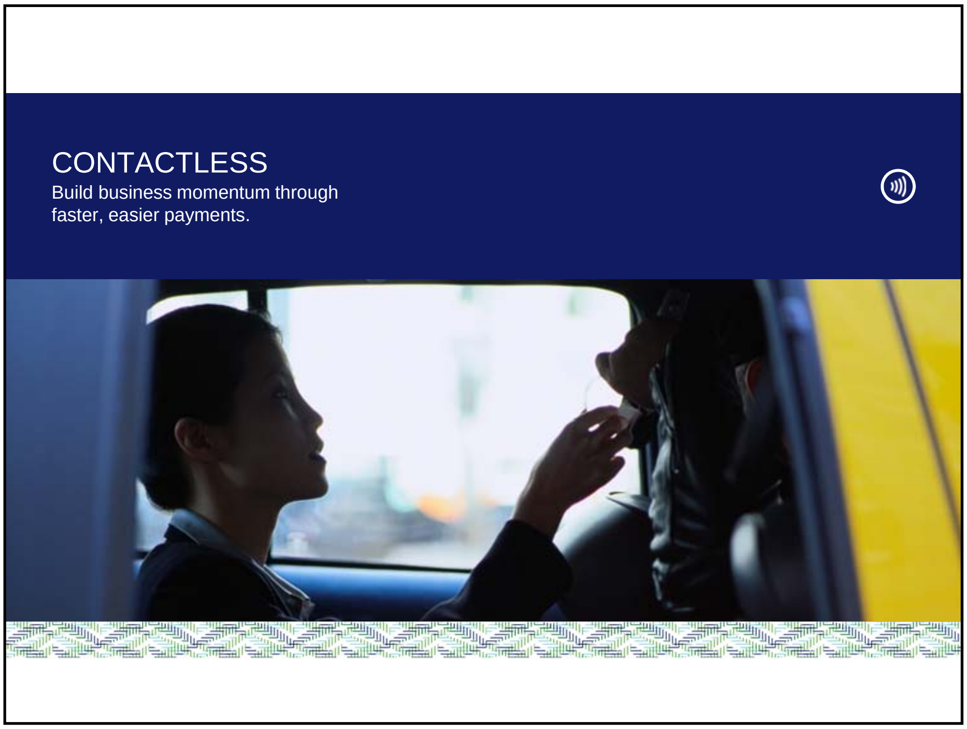
- Work with your terminal provider.
- If you connect directly with American Express, an American Express Payment Consultant can advise you.

Potential EMV Upgrade Requirements

- Upgrade POS terminal to an EMV-capable terminal.
- Ensure the terminal provider certifies the EMV-capable terminal to process American Express chip card-based transactions.
- Train employees.

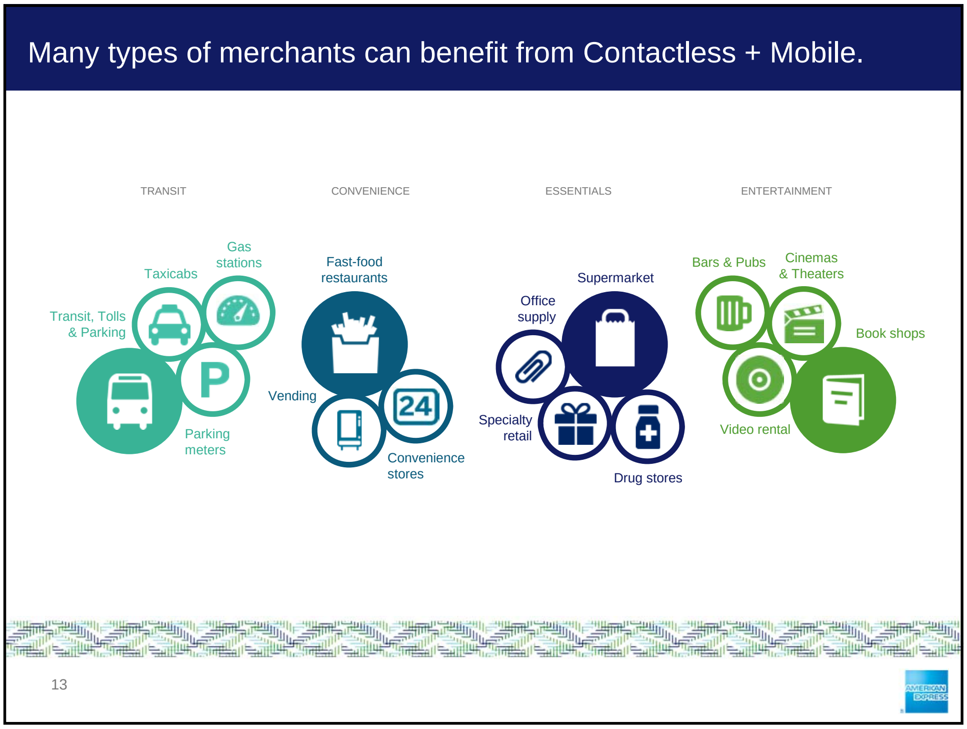
AMERICAN EXPRESS

11



CONTACTLESS

Build business momentum through faster, easier payments.



Many types of merchants can benefit from Contactless + Mobile.

TRANSIT

Gas stations

Taxicabs

Transit, Tolls & Parking

Parking meters

CONVENIENCE

Fast-food restaurants

Vending

Convenience stores

ESSENTIALS

Supermarket

Office supply

Specialty retail

Drug stores

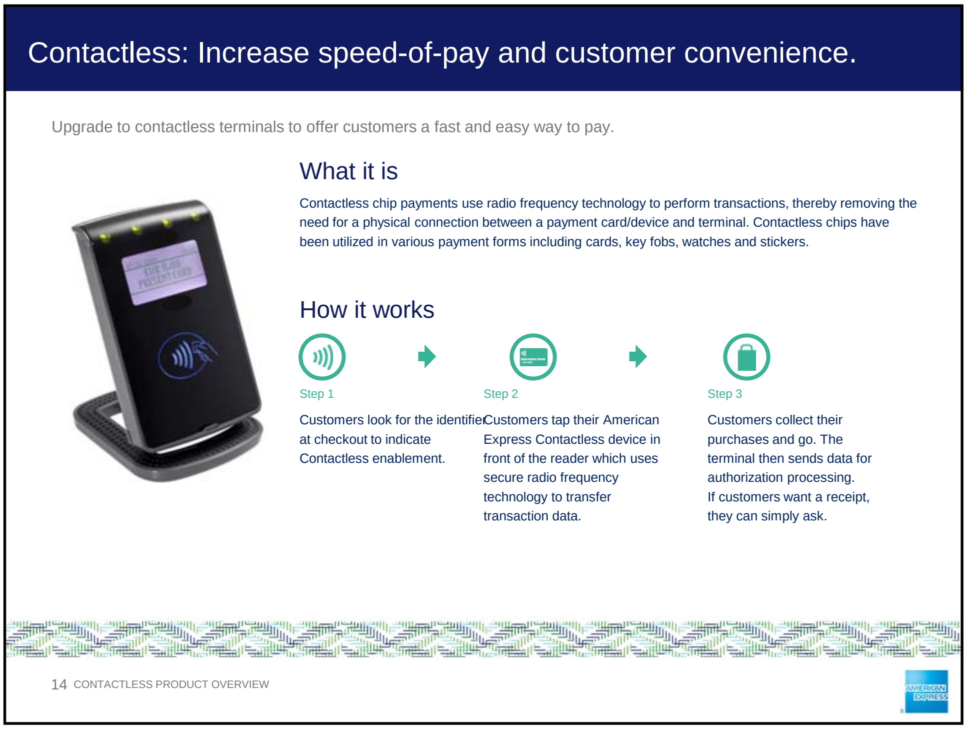
ENTERTAINMENT

Bars & Pubs

Cinemas & Theaters

Book shops

Video rental



Contactless: Increase speed-of-pay and customer convenience.

Upgrade to contactless terminals to offer customers a fast and easy way to pay.

What it is

Contactless chip payments use radio frequency technology to perform transactions, thereby removing the need for a physical connection between a payment card/device and terminal. Contactless chips have been utilized in various payment forms including cards, key fobs, watches and stickers.

How it works

Step 1

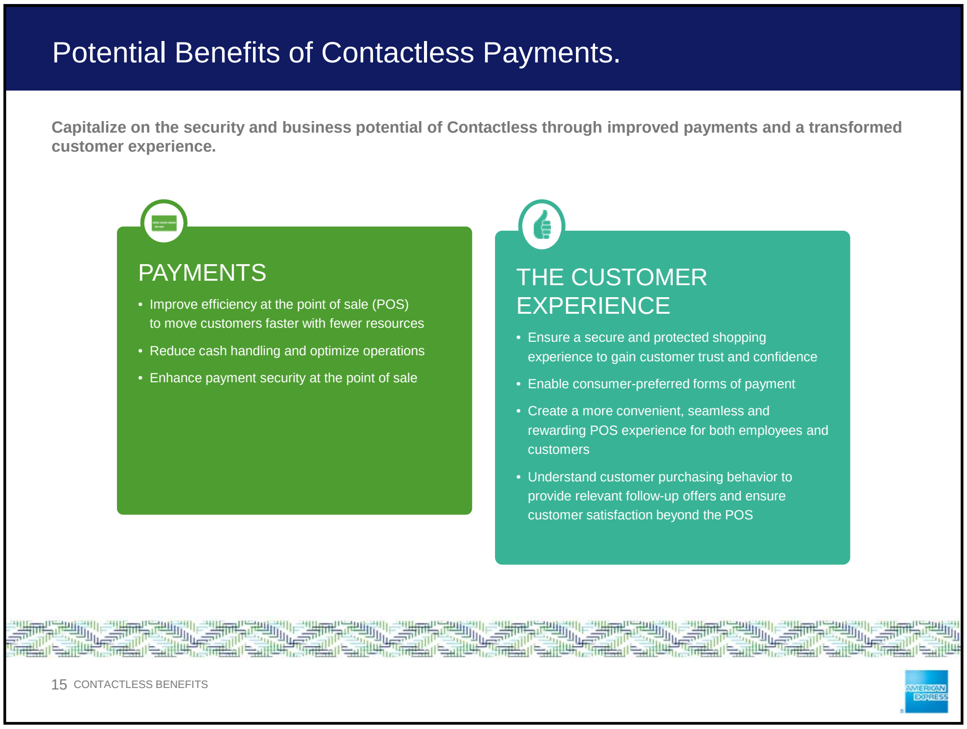
Customers look for the identifie at checkout to indicate Contactless enablement.

Step 2

Customers tap their American Express Contactless device in front of the reader which uses secure radio frequency technology to transfer transaction data.

Step 3

Customers collect their purchases and go. The terminal then sends data for authorization processing. If customers want a receipt, they can simply ask.



Potential Benefits of Contactless Payments.

Capitalize on the security and business potential of Contactless through improved payments and a transformed customer experience.

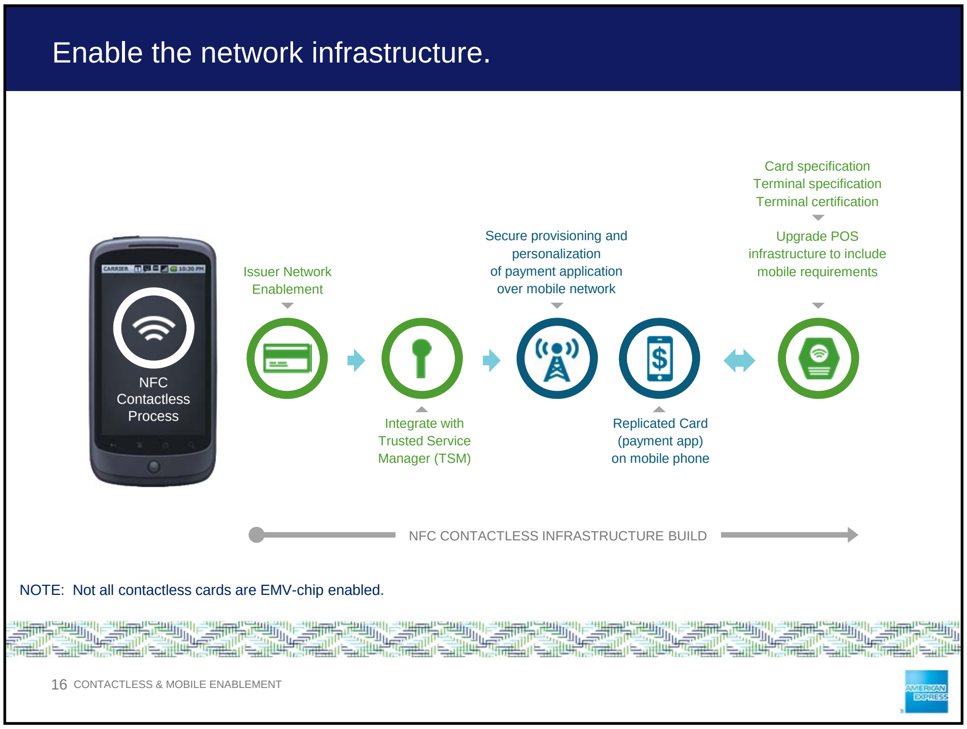
PAYMENTS

- Improve efficiency at the point of sale (POS) to move customers faster with fewer resources
- Reduce cash handling and optimize operations
- Enhance payment security at the point of sale

THE CUSTOMER EXPERIENCE

- Ensure a secure and protected shopping experience to gain customer trust and confidence
- Enable consumer-preferred forms of payment
- Create a more convenient, seamless and rewarding POS experience for both employees and customers
- Understand customer purchasing behavior to provide relevant follow-up offers and ensure customer satisfaction beyond the POS

15 CONTACTLESS BENEFITS

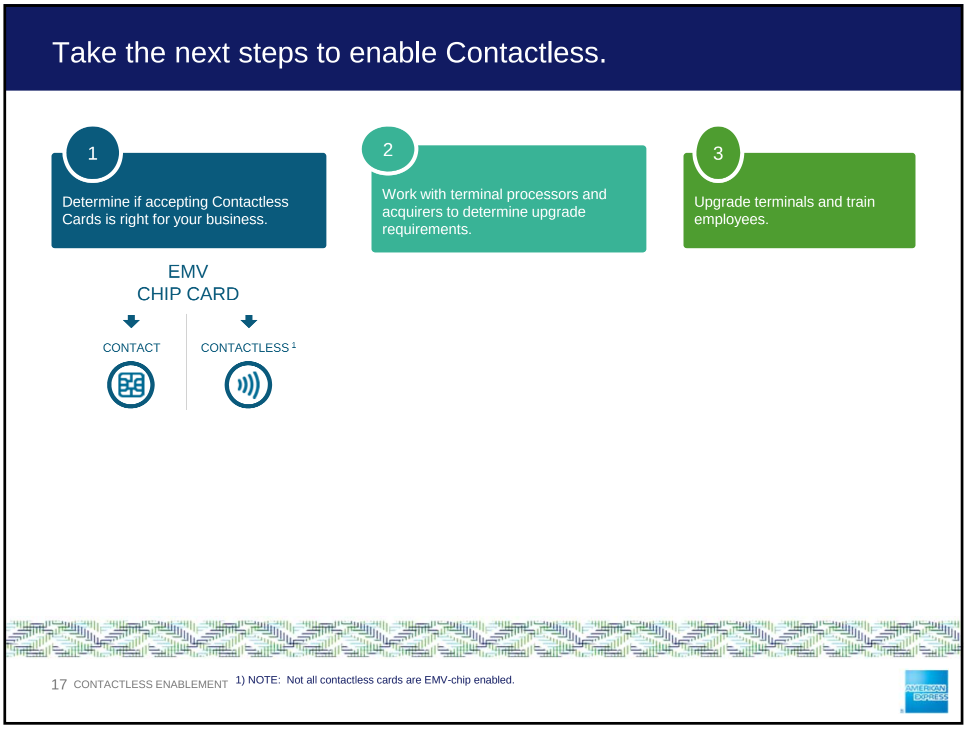


Enable the network infrastructure.

NFC Contactless Process
Issuer Network Enablement
Integrate with Trusted Service Manager (TSM)
Secure provisioning and personalization of payment application over mobile network
Replicated Card (payment app) on mobile phone
Card specification
Terminal specification
Terminal certification
Upgrade POS infrastructure to include mobile requirements
NFC CONTACTLESS INFRASTRUCTURE BUILD

NOTE: Not all contactless cards are EMV-chip enabled.

16 CONTACTLESS & MOBILE ENABLEMENT



Take the next steps to enable Contactless.

1 Determine if accepting Contactless Cards is right for your business.

2 Work with terminal processors and acquirers to determine upgrade requirements.

3 Upgrade terminals and train employees.

EMV
CHIP CARD

CONTACT

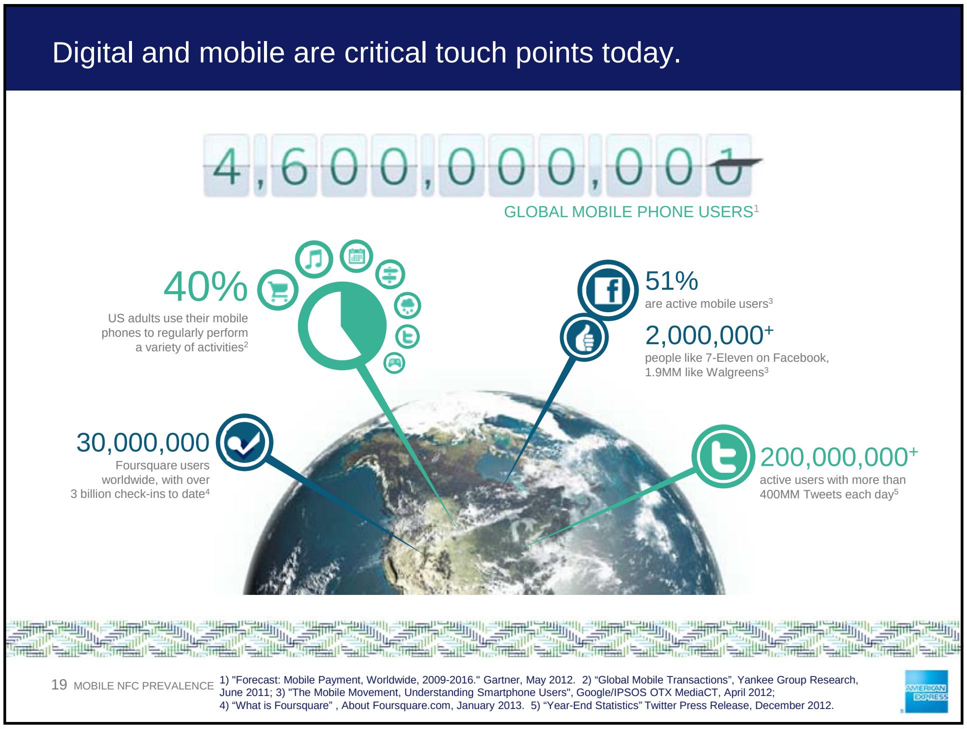
CONTACTLESS [1]

17 CONTACTLESS ENABLEMENT

[1] NOTE: Not all contactless cards are EMV-chip enabled.

MOBILE NEAR-FIELD COMMUNICATIONS (NFC)

Create richer, more meaningful
customer interactions.



Digital and mobile are critical touch points today.

4,600,000,000

GLOBAL MOBILE PHONE USERS[1]

40%
US adults use their mobile phones to regularly perform a variety of activities[2]

51%
are active mobile users[3]

2,000,000+
people like 7-Eleven on Facebook, 1.9MM like Walgreens[3]

30,000,000
Foursquare users worldwide, with over 3 billion check-ins to date[4]

200,000,000+
active users with more than 400MM Tweets each day[5]

1) "Forecast: Mobile Payment, Worldwide, 2009-2016." Gartner, May 2012. 2) “Global Mobile Transactions”, Yankee Group Research, June 2011; 3) "The Mobile Movement, Understanding Smartphone Users", Google/IPSOS OTX MediaCT, April 2012; 4) “What is Foursquare” , About Foursquare.com, January 2013. 5) “Year-End Statistics” Twitter Press Release, December 2012.

Mobile commerce is an inevitable reality.

FUTURE

119,000,000,000

MOBILE SHOPPING EXPECTED TO REACH $119B IN GLOBAL SPENDING BY 2015[1]

2013
Year smartphones expected to exceed laptops globally[2]

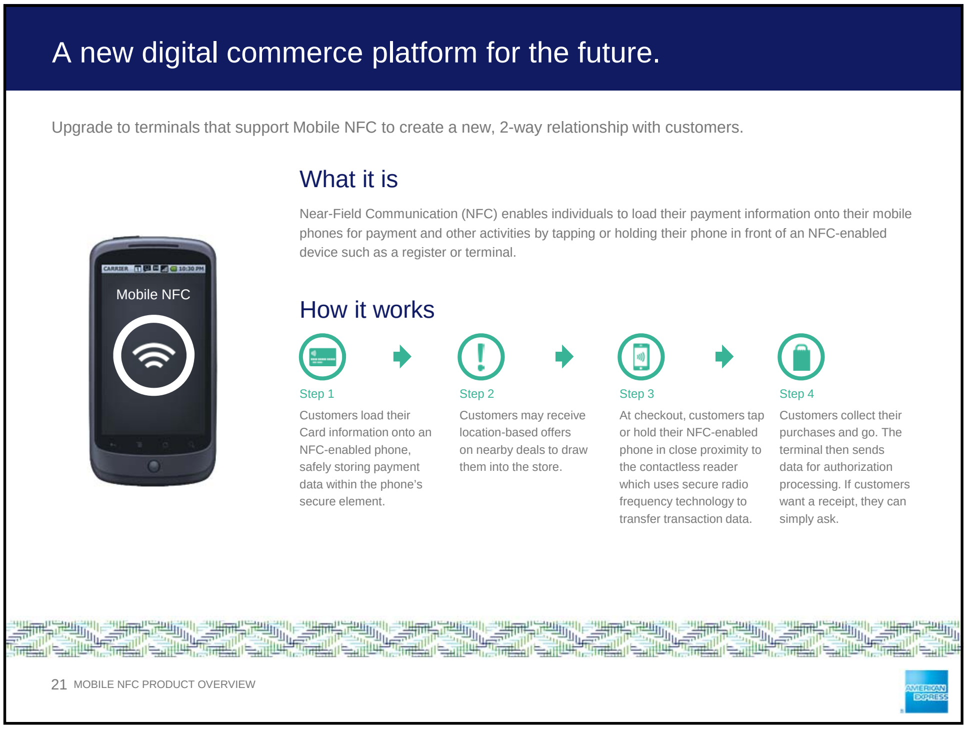
600,000,000
Expected regular mobile coupon users worldwide by 2016[4]

9 out of 10
Mobile searchers who have taken action from a smartphone search[3]

68% visit a business

53% make a purchase

1) "Mobile Commerce" study, by ABI Research, February 2012; 2) “Global Mobile Transactions”, Yankee Group Research, June 2011, 3) "The Mobile Movement, Understanding Smartphone Users", Google/IPSOS OTX MediaCT, April 2012 4) "NFC Retail Marketing & Mobile Payments" Juniper Research, April 2011.



A new digital commerce platform for the future.

Upgrade to terminals that support Mobile NFC to create a new, 2-way relationship with customers.

Mobile NFC

What it is

Near-Field Communication (NFC) enables individuals to load their payment information onto their mobile phones for payment and other activities by tapping or holding their phone in front of an NFC-enabled device such as a register or terminal.

How it works

Step 1

Customers load their Card information onto an NFC-enabled phone, safely storing payment data within the phone's secure element.

Step 2

Customers may receive location-based offers on nearby deals to draw them into the store.

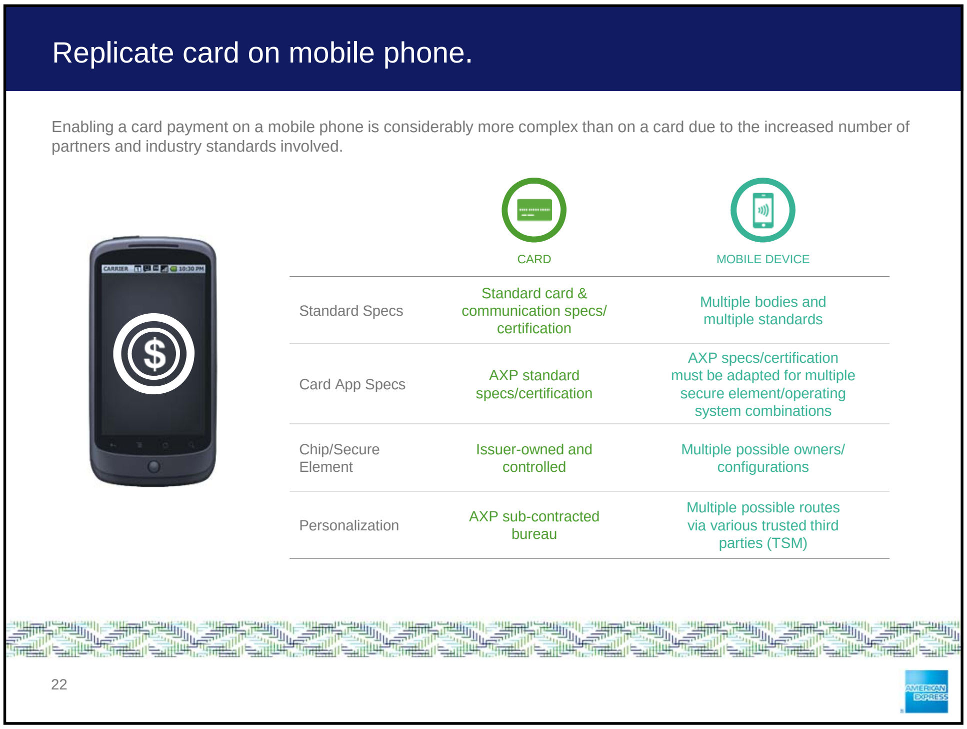
Step 3

At checkout, customers tap or hold their NFC-enabled phone in close proximity to the contactless reader which uses secure radio frequency technology to transfer transaction data.

Step 4

Customers collect their purchases and go. The terminal then sends data for authorization processing. If customers want a receipt, they can simply ask.

21 MOBILE NFC PRODUCT OVERVIEW

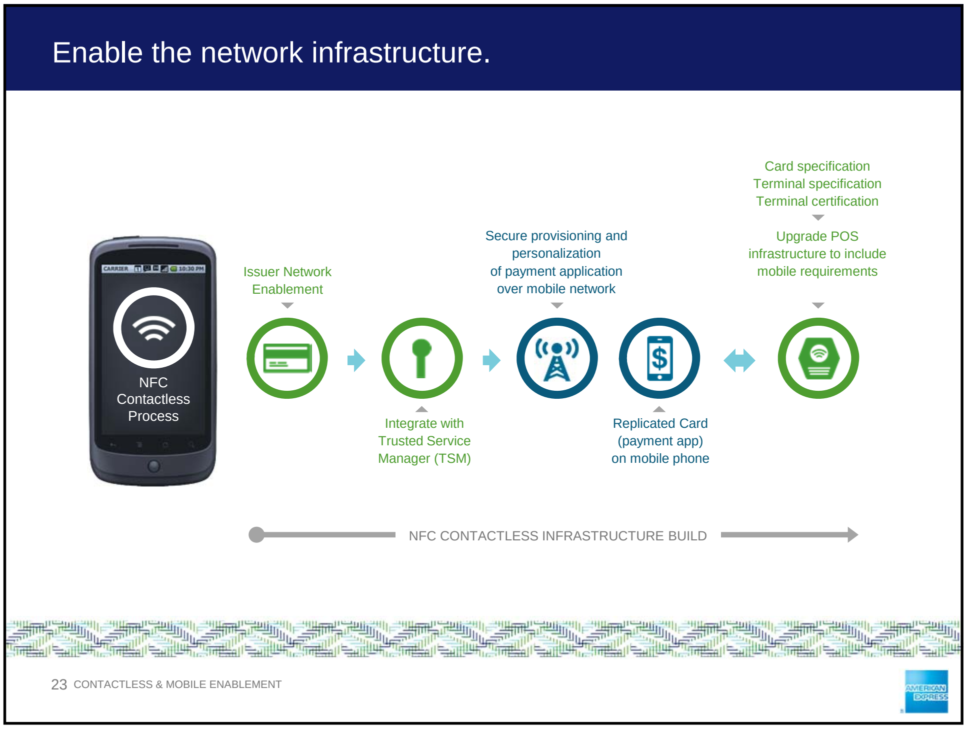


Replicate card on mobile phone.

Enabling a card payment on a mobile phone is considerably more complex than on a card due to the increased number of partners and industry standards involved.

	CARD	MOBILE DEVICE
Standard Specs	Standard card & communication specs/ certification	Multiple bodies and multiple standards
Card App Specs	AXP standard specs/certification	AXP specs/certification must be adapted for multiple secure element/operating system combinations
Chip/Secure Element	Issuer-owned and controlled	Multiple possible owners/ configurations
Personalization	AXP sub-contracted bureau	Multiple possible routes via various trusted third parties (TSM)

22



Enable the network infrastructure.

NFC Contactless Process

Issuer Network Enablement

Integrate with Trusted Service Manager (TSM)

Secure provisioning and personalization of payment application over mobile network

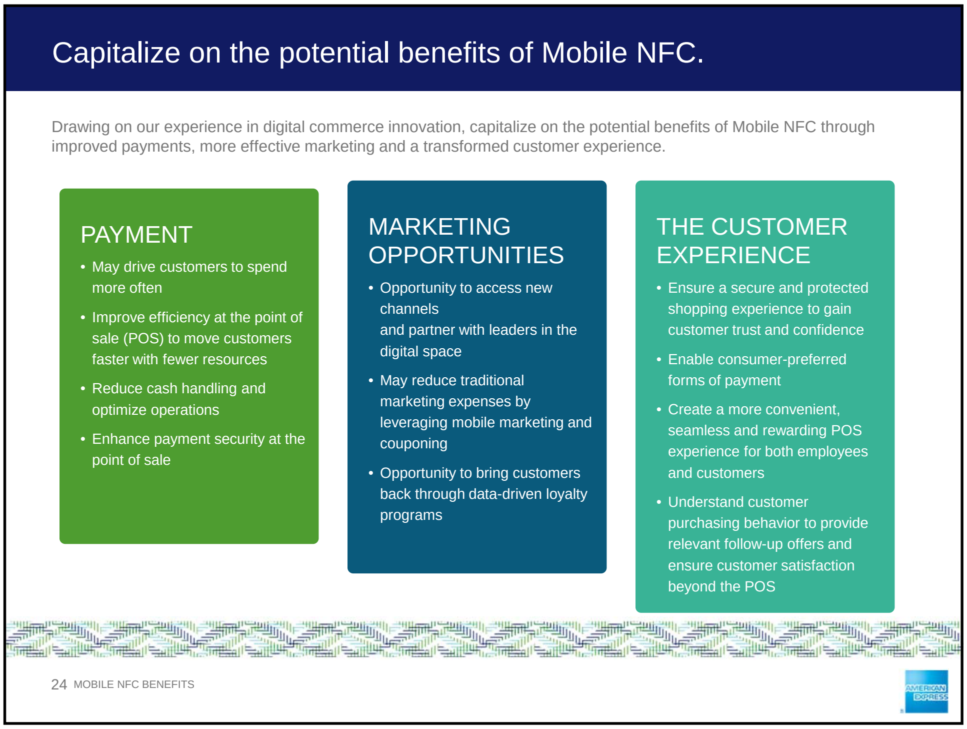
Replicated Card (payment app) on mobile phone

Card specification
Terminal specification
Terminal certification

Upgrade POS infrastructure to include mobile requirements

NFC CONTACTLESS INFRASTRUCTURE BUILD

23 CONTACTLESS & MOBILE ENABLEMENT



Capitalize on the potential benefits of Mobile NFC.

Drawing on our experience in digital commerce innovation, capitalize on the potential benefits of Mobile NFC through improved payments, more effective marketing and a transformed customer experience.

PAYMENT

- May drive customers to spend more often
- Improve efficiency at the point of sale (POS) to move customers faster with fewer resources
- Reduce cash handling and optimize operations
- Enhance payment security at the point of sale

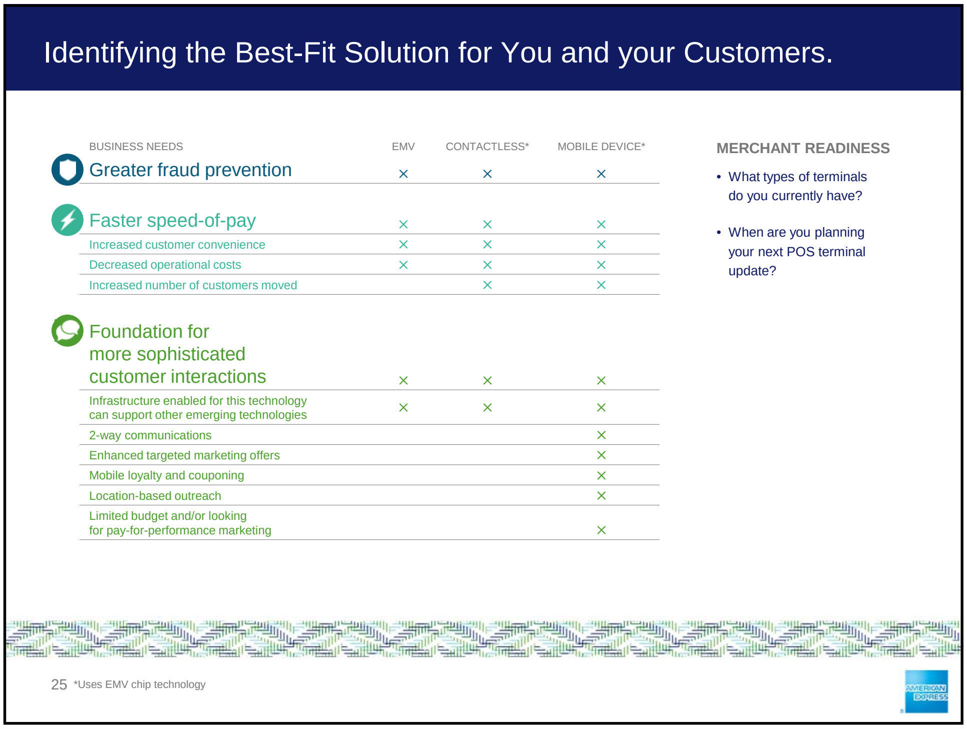
MARKETING OPPORTUNITIES

- Opportunity to access new channels and partner with leaders in the digital space
- May reduce traditional marketing expenses by leveraging mobile marketing and couponing
- Opportunity to bring customers back through data-driven loyalty programs

THE CUSTOMER EXPERIENCE

- Ensure a secure and protected shopping experience to gain customer trust and confidence
- Enable consumer-preferred forms of payment
- Create a more convenient, seamless and rewarding POS experience for both employees and customers
- Understand customer purchasing behavior to provide relevant follow-up offers and ensure customer satisfaction beyond the POS

24 MOBILE NFC BENEFITS



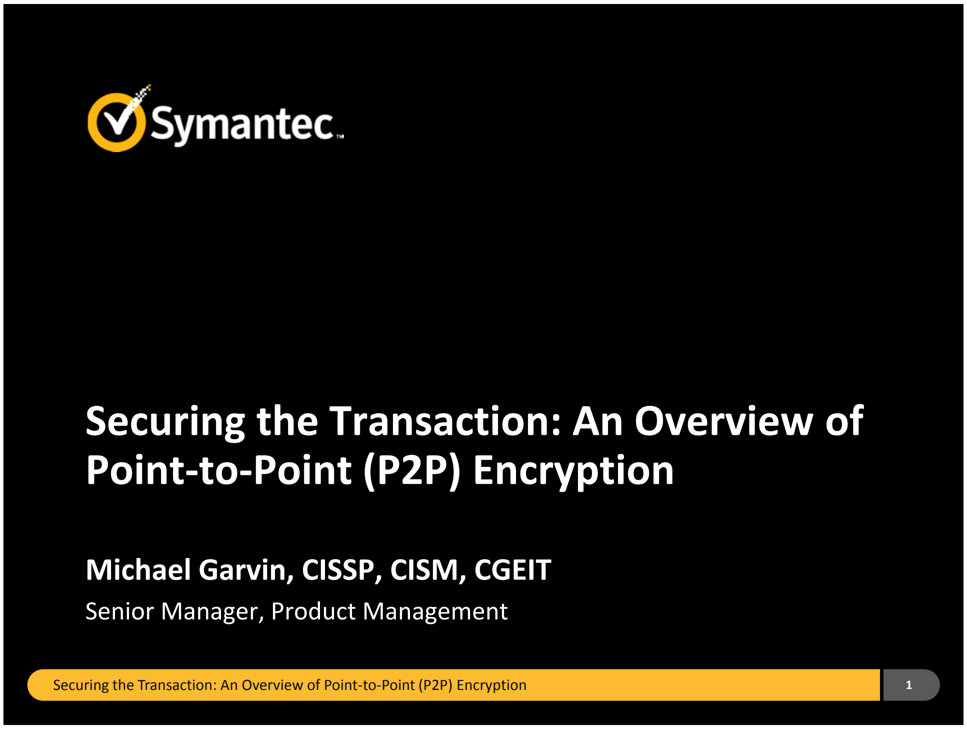
Identifying the Best-Fit Solution for You and your Customers.

BUSINESS NEEDS	EMV	CONTACTLESS*	MOBILE DEVICE*
Greater fraud prevention	×	×	×
Faster speed-of-pay	×	×	×
Increased customer convenience	×	×	×
Decreased operational costs	×	×	×
Increased number of customers moved		×	×
Foundation for more sophisticated customer interactions	×	×	×
Infrastructure enabled for this technology can support other emerging technologies	×	×	×
2-way communications			×
Enhanced targeted marketing offers			×
Mobile loyalty and couponing			×
Location-based outreach			×
Limited budget and/or looking for pay-for-performance marketing			×

MERCHANT READINESS

- What types of terminals do you currently have?
- When are you planning your next POS terminal update?

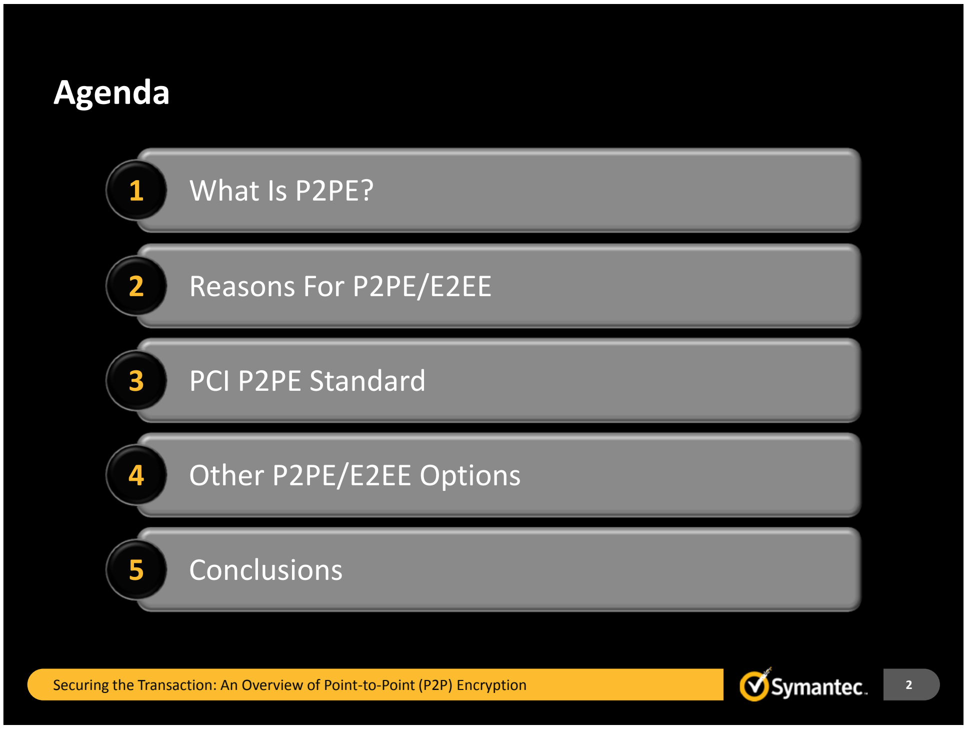
*Uses EMV chip technology



Securing the Transaction: An Overview of Point-to-Point (P2P) Encryption

Michael Garvin, CISSP, CISM, CGEIT

Senior Manager, Product Management



Agenda

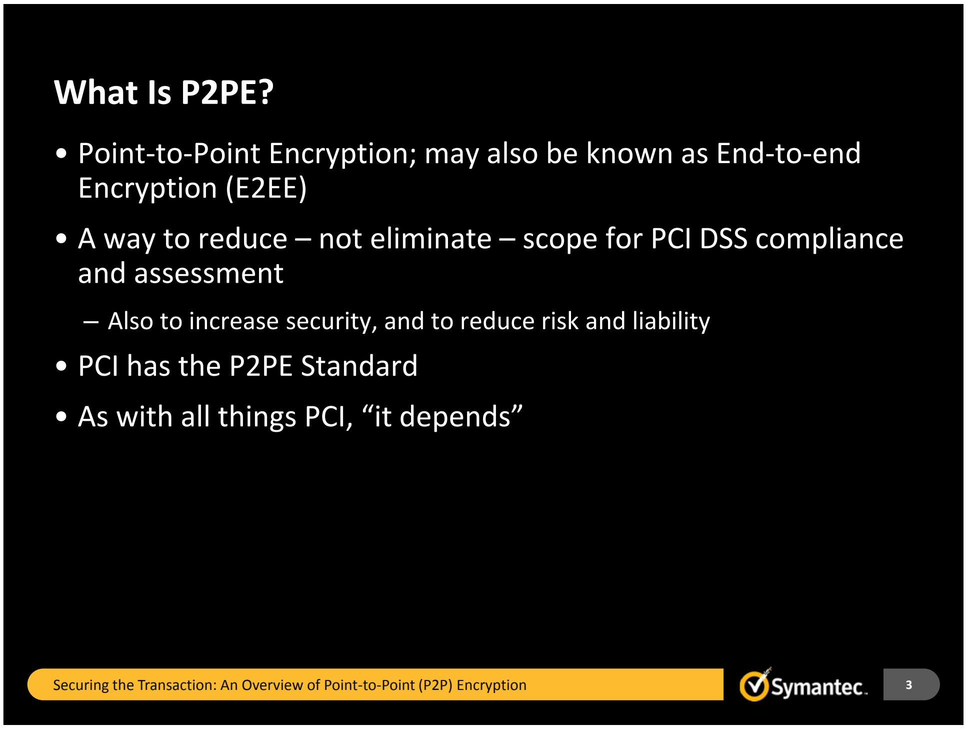
1 What Is P2PE?

2 Reasons For P2PE/E2EE

3 PCI P2PE Standard

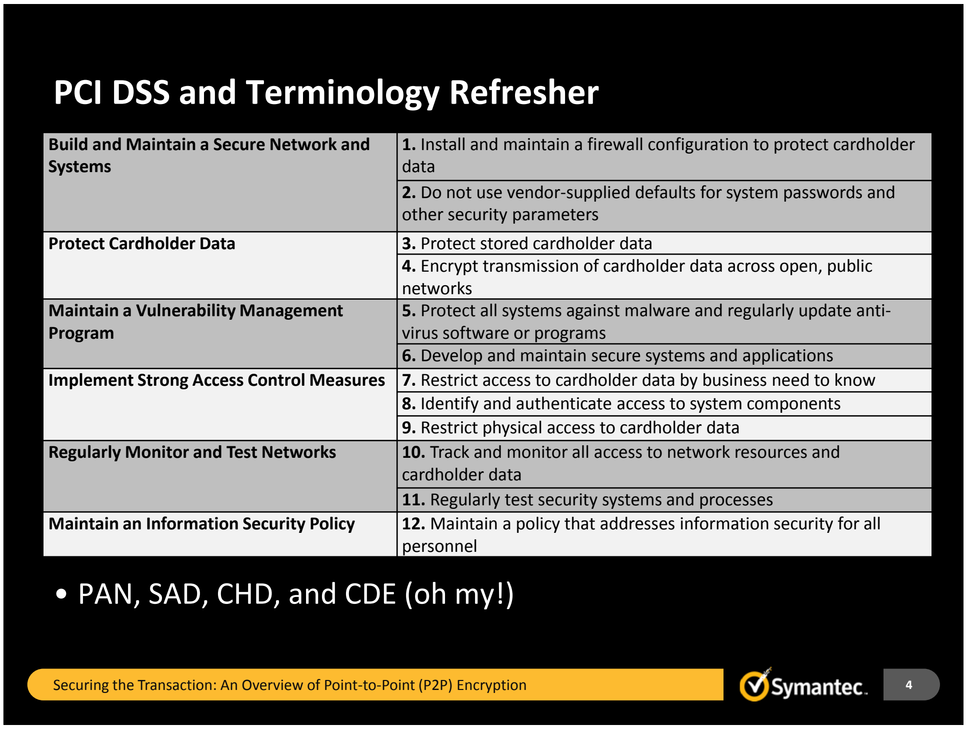
4 Other P2PE/E2EE Options

5 Conclusions



What Is P2PE?

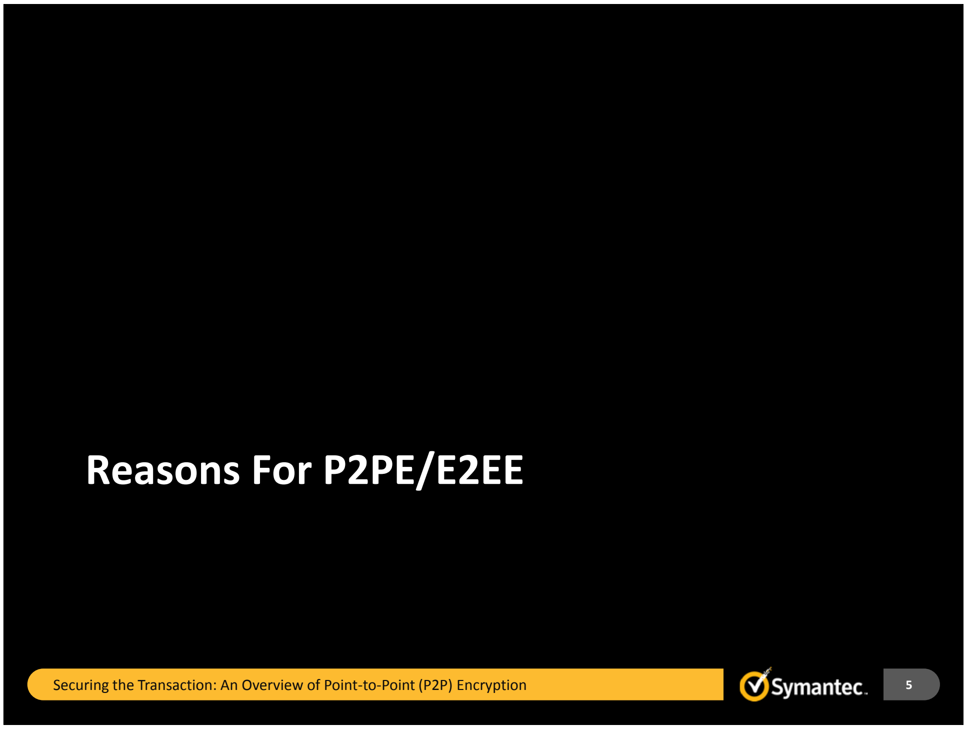
- Point-to-Point Encryption; may also be known as End-to-end Encryption (E2EE)
- A way to reduce – not eliminate – scope for PCI DSS compliance and assessment
  - Also to increase security, and to reduce risk and liability
- PCI has the P2PE Standard
- As with all things PCI, “it depends”



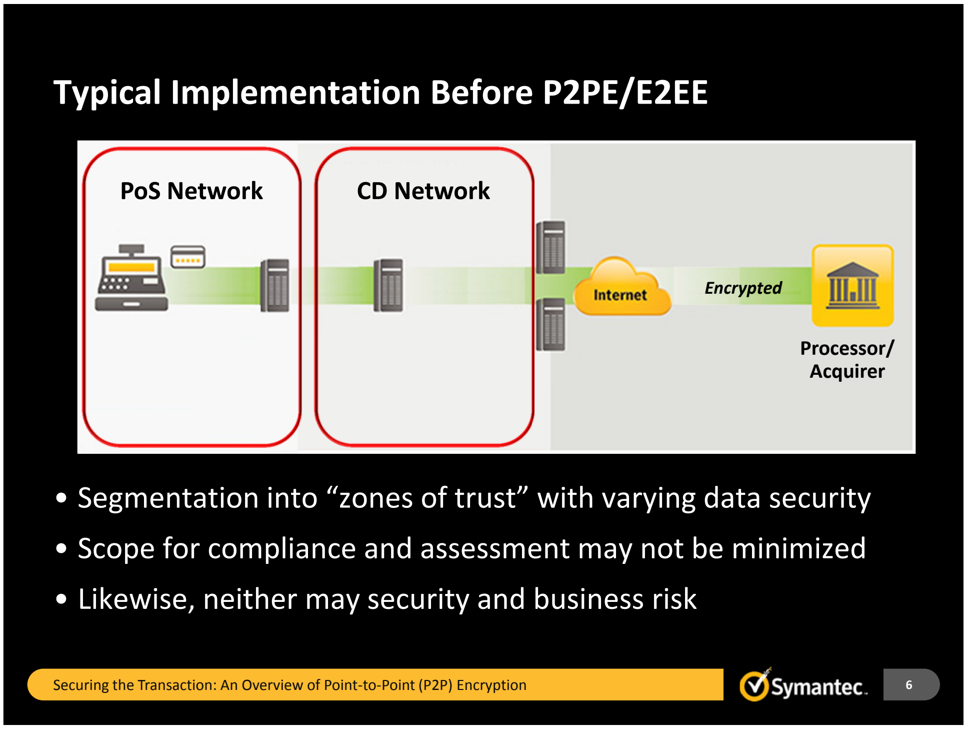
PCI DSS and Terminology Refresher

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

- PAN, SAD, CHD, and CDE (oh my!)



Reasons For P2PE/E2EE



Typical Implementation Before P2PE/E2EE

PoS Network

CD Network

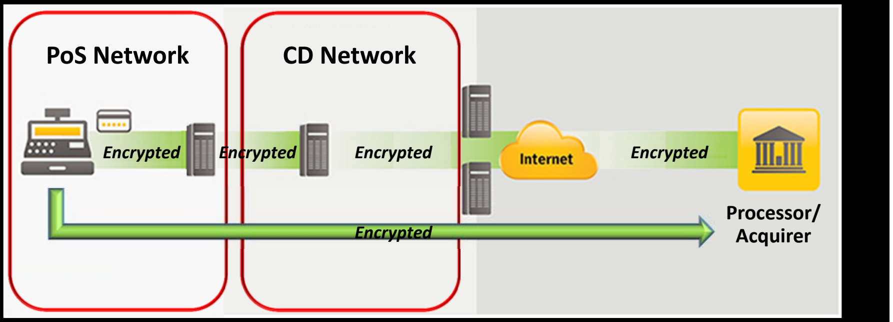
Internet

Encrypted

Processor/ Acquirer

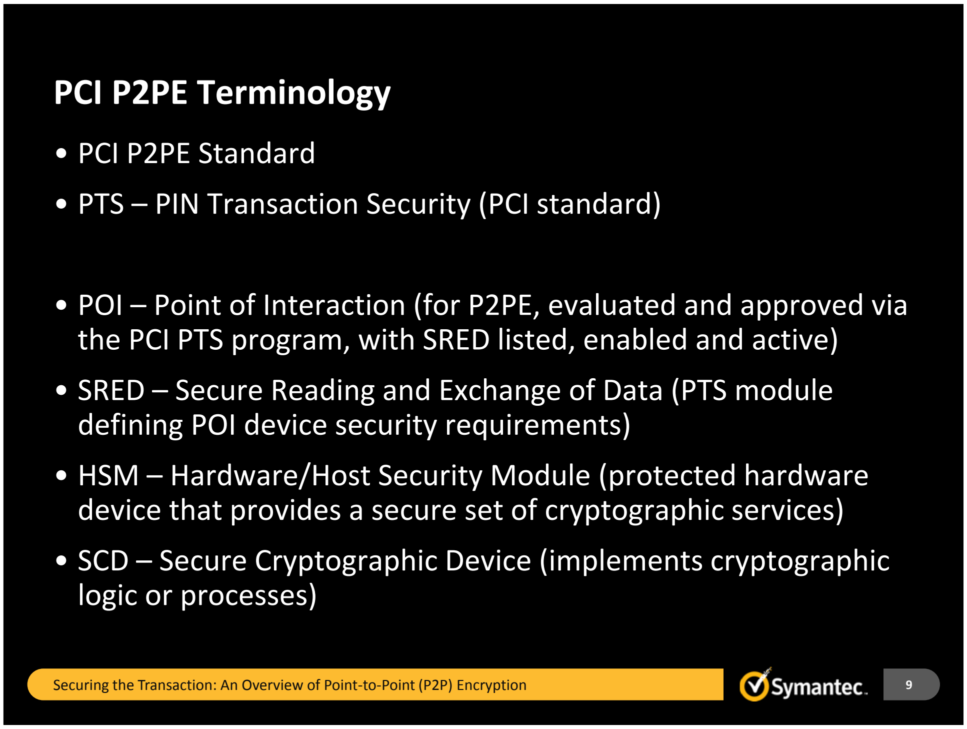
- Segmentation into “zones of trust” with varying data security
- Scope for compliance and assessment may not be minimized
- Likewise, neither may security and business risk

Implementation With P2PE/E2EE



- Encrypted data flows through existing channels, or is sent directly to a service provider
- Organization has limited/no ability to decrypt cardholder data
- Scope is limited, risks are reduced

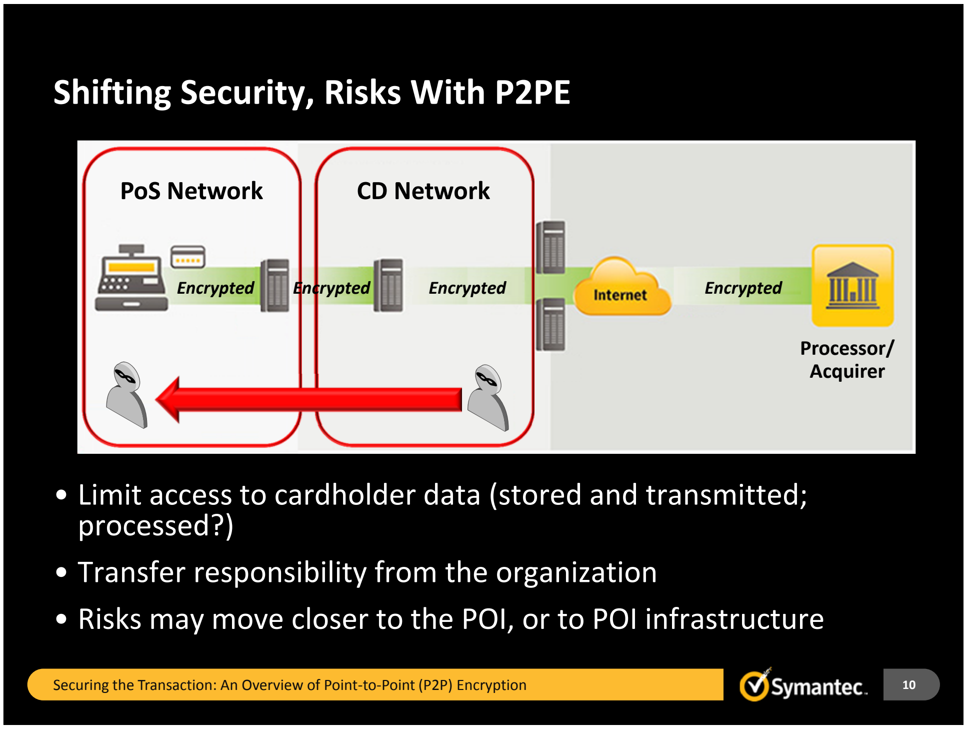
PCI P2PE Standard



PCI P2PE Terminology

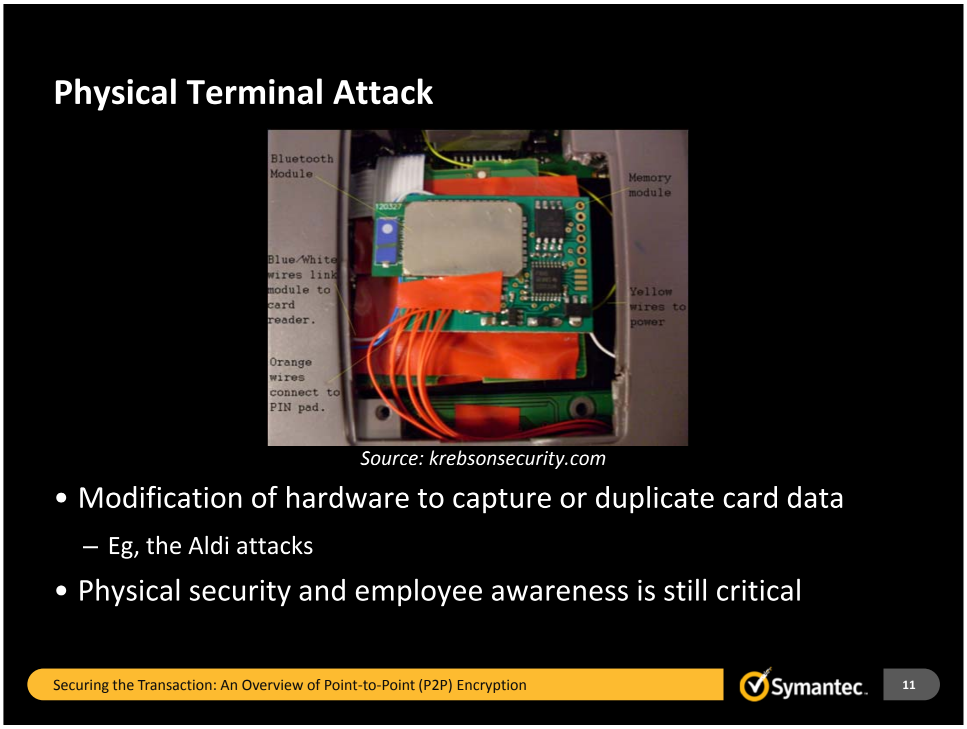
- PCI P2PE Standard
- PTS – PIN Transaction Security (PCI standard)

- POI – Point of Interaction (for P2PE, evaluated and approved via the PCI PTS program, with SRED listed, enabled and active)
- SRED – Secure Reading and Exchange of Data (PTS module defining POI device security requirements)
- HSM – Hardware/Host Security Module (protected hardware device that provides a secure set of cryptographic services)
- SCD – Secure Cryptographic Device (implements cryptographic logic or processes)



Shifting Security, Risks With P2PE

- Limit access to cardholder data (stored and transmitted; processed?)
- Transfer responsibility from the organization
- Risks may move closer to the POI, or to POI infrastructure

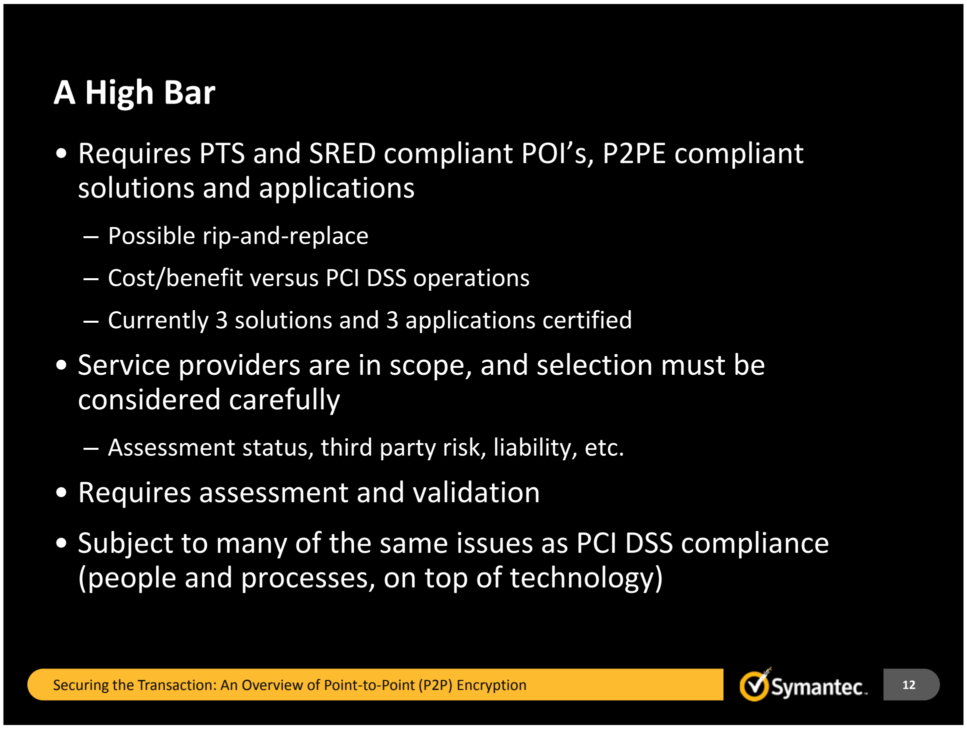


Physical Terminal Attack

Bluetooth Module
120327
Memory module
Blue/White wires link module to card reader.
Yellow wires to power
Orange wires connect to PIN pad.

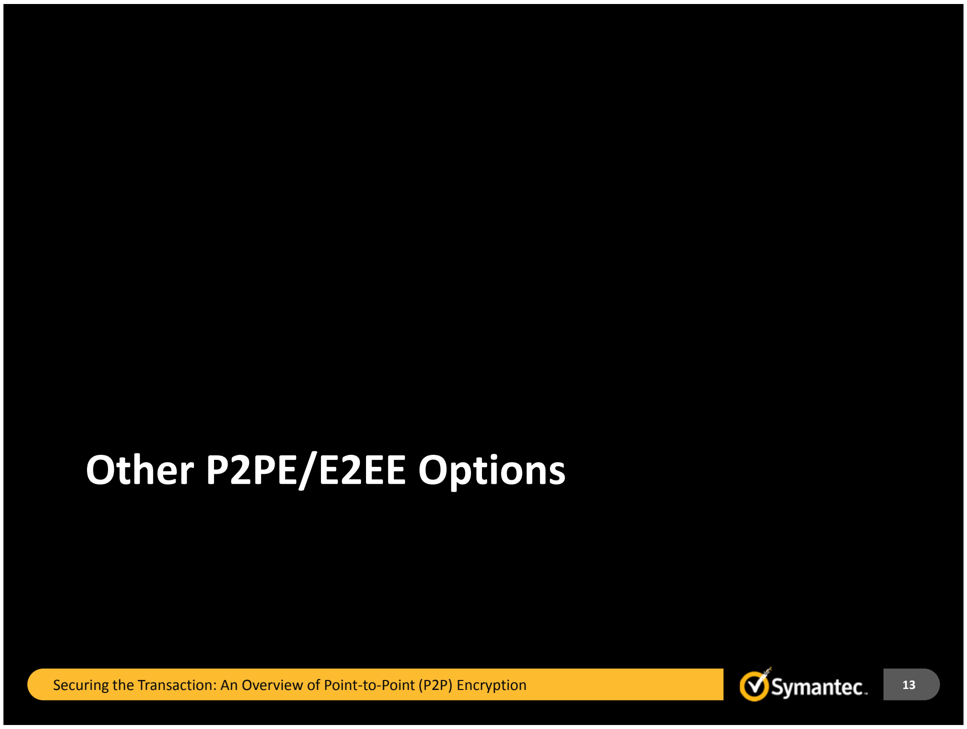
Source: krebsonsecurity.com

- Modification of hardware to capture or duplicate card data
  - Eg, the Aldi attacks
- Physical security and employee awareness is still critical

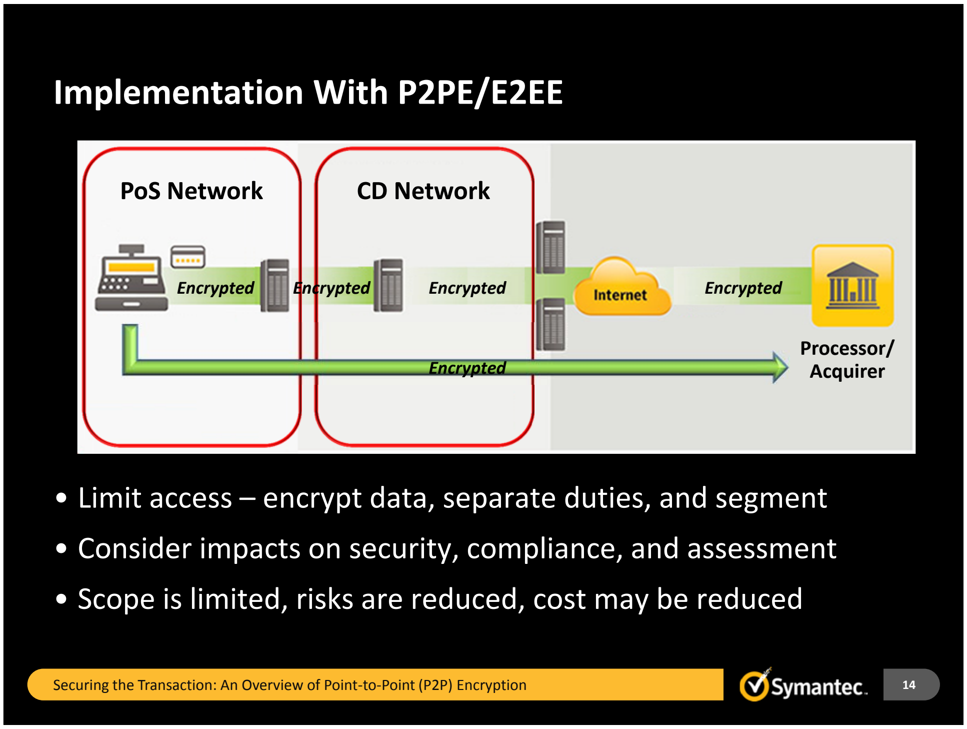


A High Bar

- Requires PTS and SRED compliant POI's, P2PE compliant solutions and applications
  - Possible rip-and-replace
  - Cost/benefit versus PCI DSS operations
  - Currently 3 solutions and 3 applications certified
- Service providers are in scope, and selection must be considered carefully
  - Assessment status, third party risk, liability, etc.
- Requires assessment and validation
- Subject to many of the same issues as PCI DSS compliance (people and processes, on top of technology)



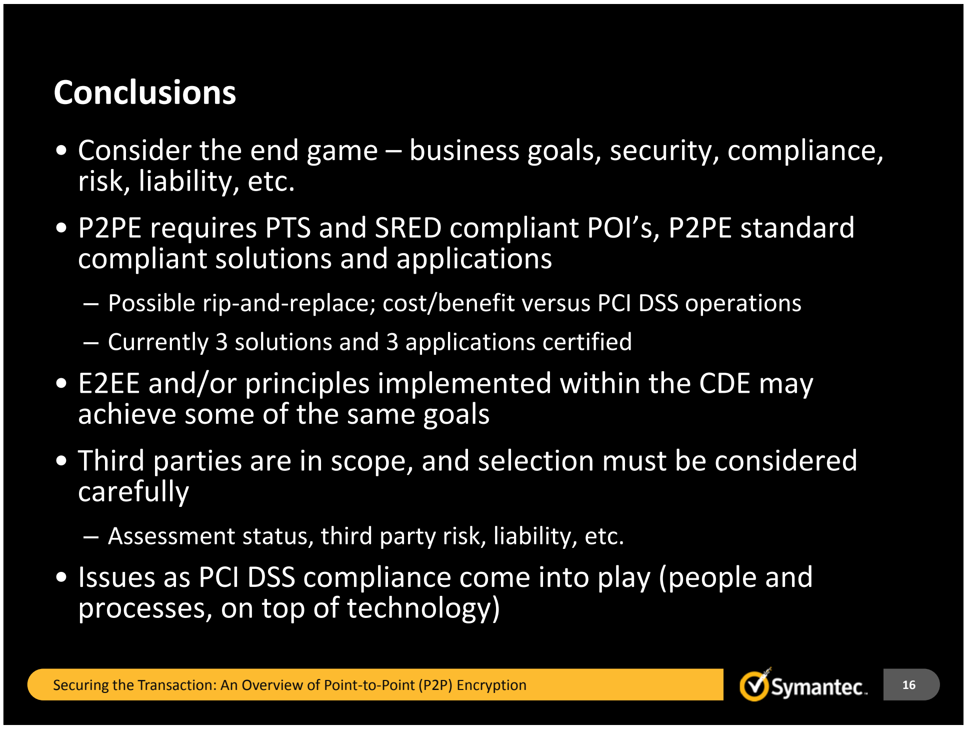
Other P2PE/E2EE Options



Implementation With P2PE/E2EE

- Limit access – encrypt data, separate duties, and segment
- Consider impacts on security, compliance, and assessment
- Scope is limited, risks are reduced, cost may be reduced

Conclusions



Conclusions

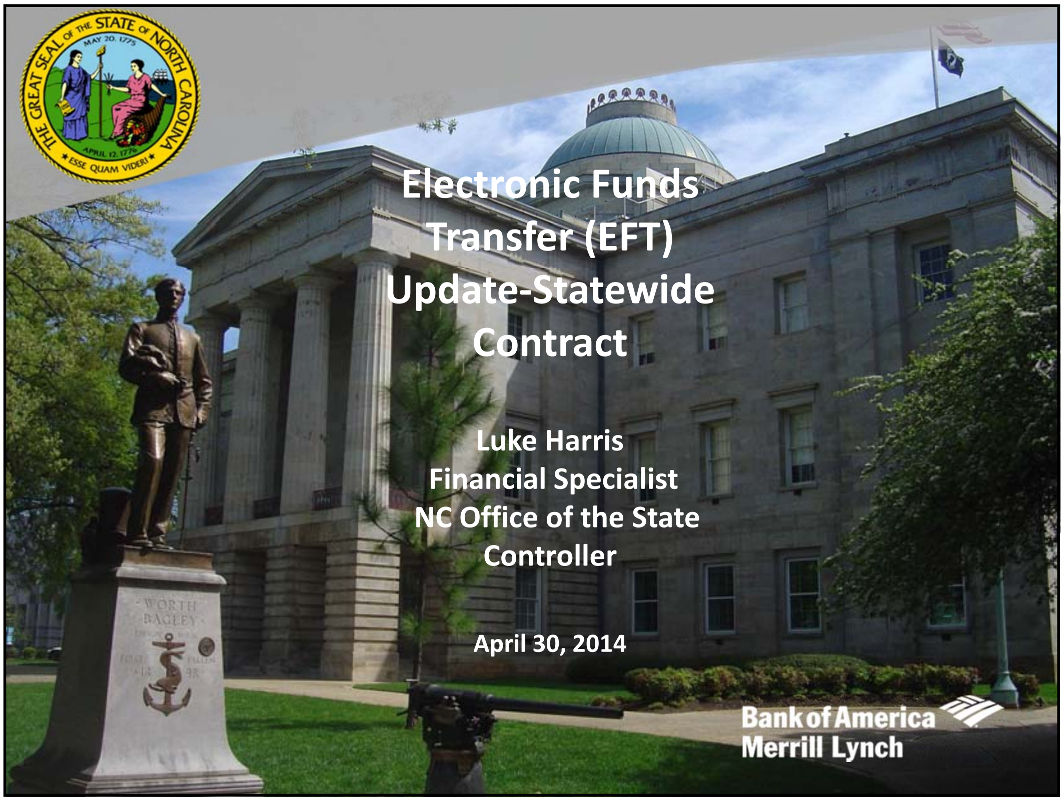
- Consider the end game – business goals, security, compliance, risk, liability, etc.
- P2PE requires PTS and SRED compliant POI's, P2PE standard compliant solutions and applications
  - Possible rip-and-replace; cost/benefit versus PCI DSS operations
  - Currently 3 solutions and 3 applications certified
- E2EE and/or principles implemented within the CDE may achieve some of the same goals
- Third parties are in scope, and selection must be considered carefully
  - Assessment status, third party risk, liability, etc.
- Issues as PCI DSS compliance come into play (people and processes, on top of technology)

Symantec.

Thank you!

Michael Garvin, CISSP, CISM, CGEIT
Senior Manager, Product Management
michael_garvin@symantec.com

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

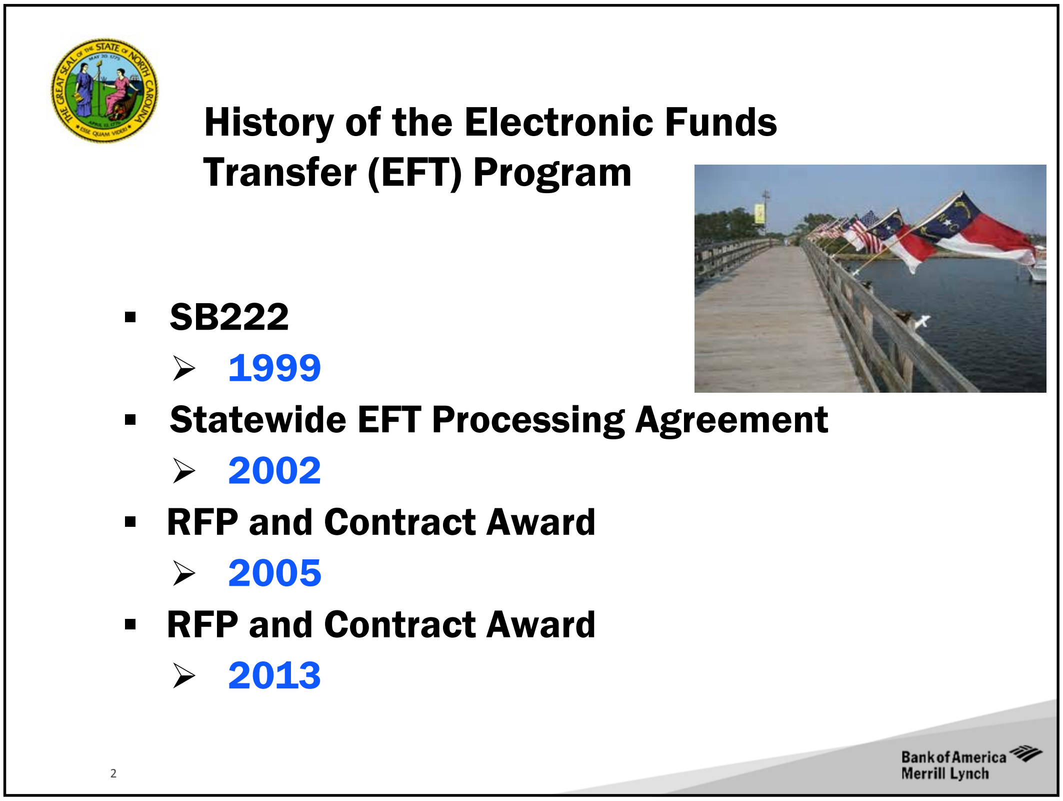


Electronic Funds Transfer (EFT) Update-Statewide Contract

Luke Harris
Financial Specialist
NC Office of the State Controller

April 30, 2014

Bank of America
Merrill Lynch



History of the Electronic Funds Transfer (EFT) Program

- SB222
  - 1999
- Statewide EFT Processing Agreement
  - 2002
- RFP and Contract Award
  - 2005
- RFP and Contract Award
  - 2013

2

Bank of America
Merrill Lynch

Timeline of EFT 2013 Contract Award and Conversion

- Contract Awarded
  - ➢ June 2013
- Memo Announcing Award
  - ➢ July 2013
- Initial Stakeholder Meeting
  - ➢ August 2013
- Second Stakeholder Meeting
  - ➢ September 2013

3

Bank of America Merrill Lynch

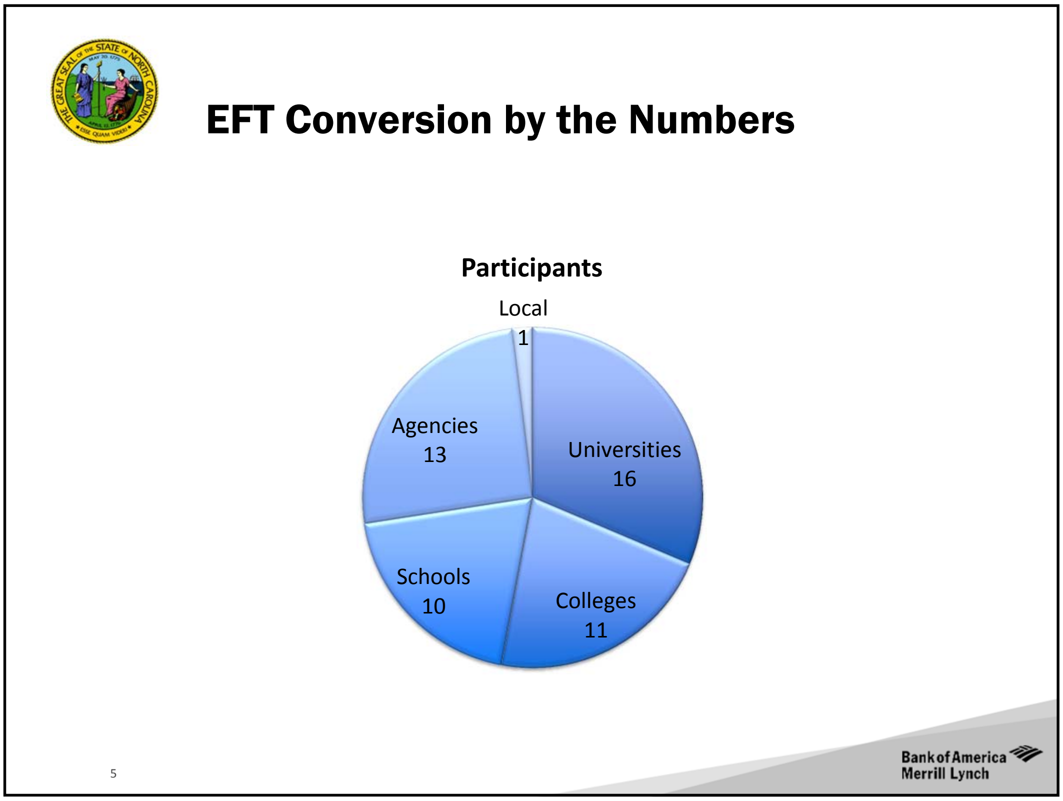
Timeline of EFT 2013 Contract Award and Conversion - continued

- Conversion schedule
  - ➢ September 2013

  Phase II stakeholder meeting
  - ➢ September 2013
- NCAS Vendor Payments & HR Payroll (Pilots)
  - ➢ October 2013
- Target conversion date
  - ➢ April 2014

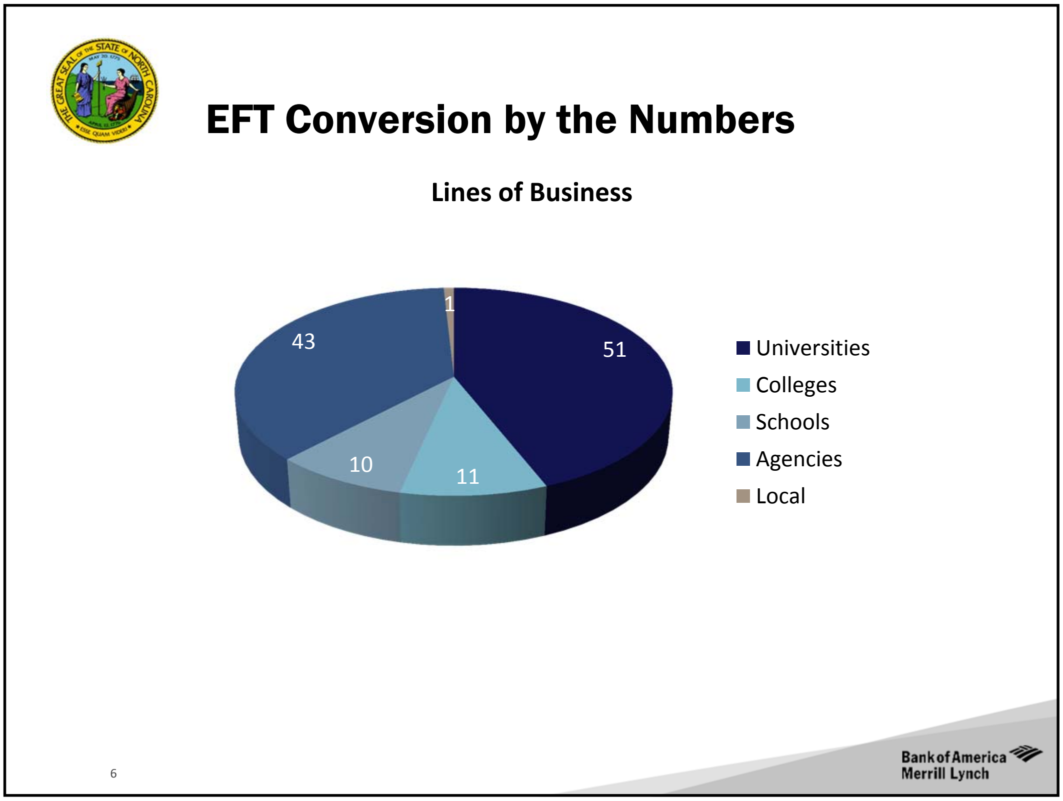
4

Bank of America Merrill Lynch



EFT Conversion by the Numbers

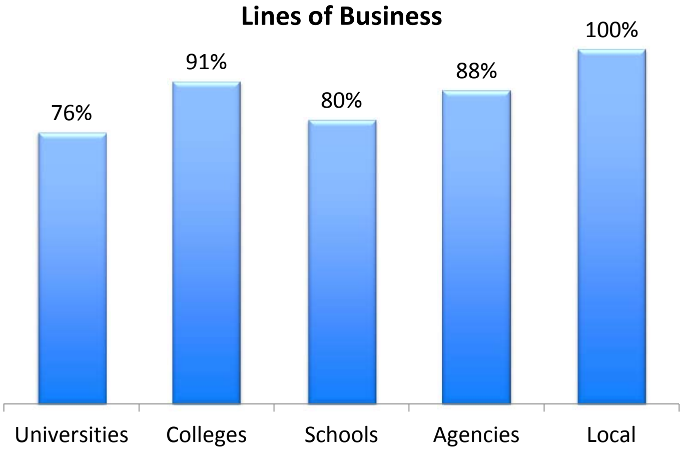
Bank of America Merrill Lynch



EFT Conversion by the Numbers

Bank of America Merrill Lynch

EFT Conversion by the Numbers



7

Bank of America Merrill Lynch

Office of the State Controller 2014 eCommerce Conference

Prepaid Card Solutions

Doris N. Dixon, Director, Senior Prepaid Card Specialist

April 30, 2014

Bank of America Merrill Lynch

Credit vs. Debit vs. Prepaid

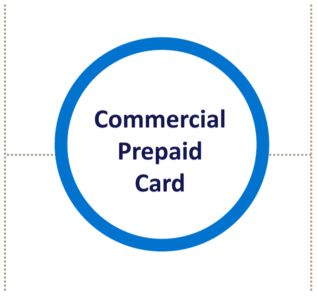
Bank of America Merrill Lynch

Credit	Debit	Prepaid
Pay Later	***Pay Now***	***Pay Before***
Credit extension	Tied to directly to your Checking Account	Pre-funded/No credit

9

Prepaid has many features

Bank of America Merrill Lynch



Consumer payments

Business Expense

Reloadable

Commercial Prepaid Card

Non-reloadable

Cash access

Purchases only

Prepaid debit card programs can save the government and higher education institutions money and enhanced client service in a number of ways. The programs made it possible to make electronic payments to those without bank accounts, they are widely-accepted by retailers, they provide added security for cardholders and they provide widespread access to cash.

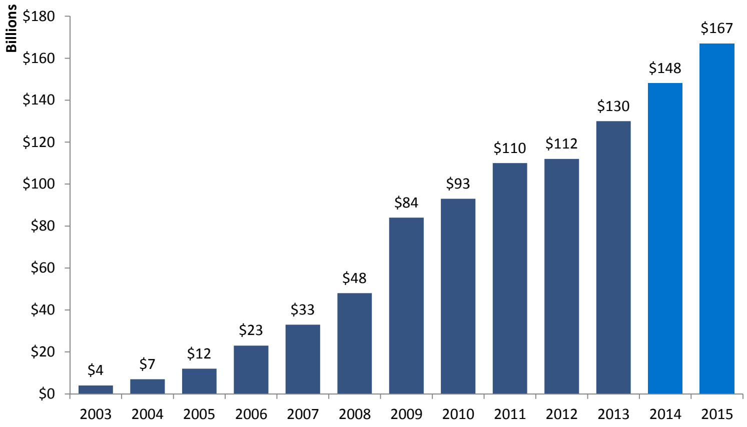
10

Current payment trends research

While prepaid cards gain in popularity…

Bank of America Merrill Lynch

Total dollars loaded onto open-loop Commercial Prepaid Cards in the U.S.



*By 2015, the industry expects a **55%** increase in total dollars loaded onto commercial prepaid cards since 2010 alone.

Note: Includes dollars loaded in the open-loop segments of:

- Events & Meetings
- Employee & Partner Incentives
- Consumer Incentives
- Campus
- Social Security
- TANF
- Transit
- State Unemployment, Insurance
- Payroll
- Benefits
- FSA/HAS

Prepaid Card trends

Bank of America Merrill Lynch

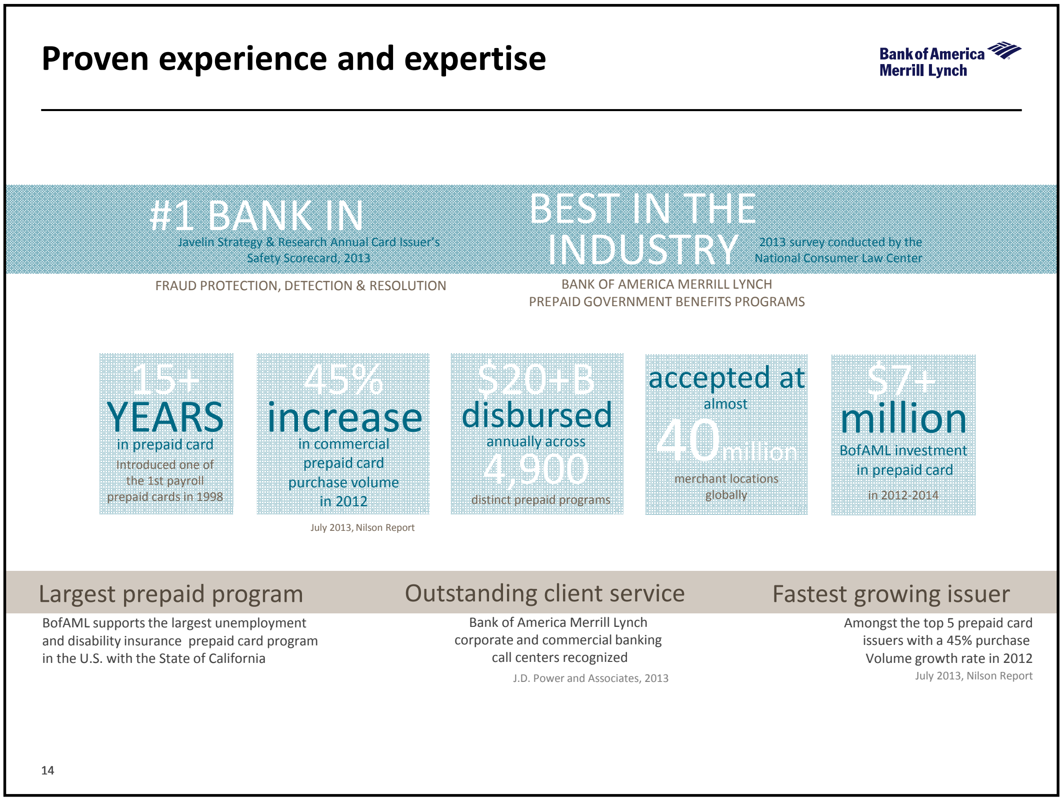
- Card recipients have demonstrated a strong preference for cards over cash and are quickly becoming one the most popular payment methods
- New research indicates that prepaid cards are quickly becoming a viable alternative to checks, cash rewards and merchandise offers

*Governments and the recipients of government payments derive significant benefits by using prepaid debit cards in lieu of paper checks.

Bank of America Merrill Lynch offers a variety of turn-key prepaid solutions for government, employee and consumer payments that reduce costs, streamline operations and better meet the recipients needs.

Prepaid Solutions

Bank of America
Merrill Lynch



Proven experience and expertise

Bank of America
Merrill Lynch

#1 BANK IN
Javelin Strategy & Research Annual Card Issuer's Safety Scorecard, 2013
FRAUD PROTECTION, DETECTION & RESOLUTION

BEST IN THE INDUSTRY
2013 survey conducted by the National Consumer Law Center
BANK OF AMERICA MERRILL LYNCH PREPAID GOVERNMENT BENEFITS PROGRAMS

15+ YEARS in prepaid card
Introduced one of the 1st payroll prepaid cards in 1998

45% increase in commercial prepaid card purchase volume in 2012
July 2013, Nilson Report

$20+B disbursed annually across 4,900 distinct prepaid programs

accepted at almost 40 million merchant locations globally

$7+ million BofAML investment in prepaid card in 2012-2014

Largest prepaid program

BofAML supports the largest unemployment and disability insurance prepaid card program in the U.S. with the State of California

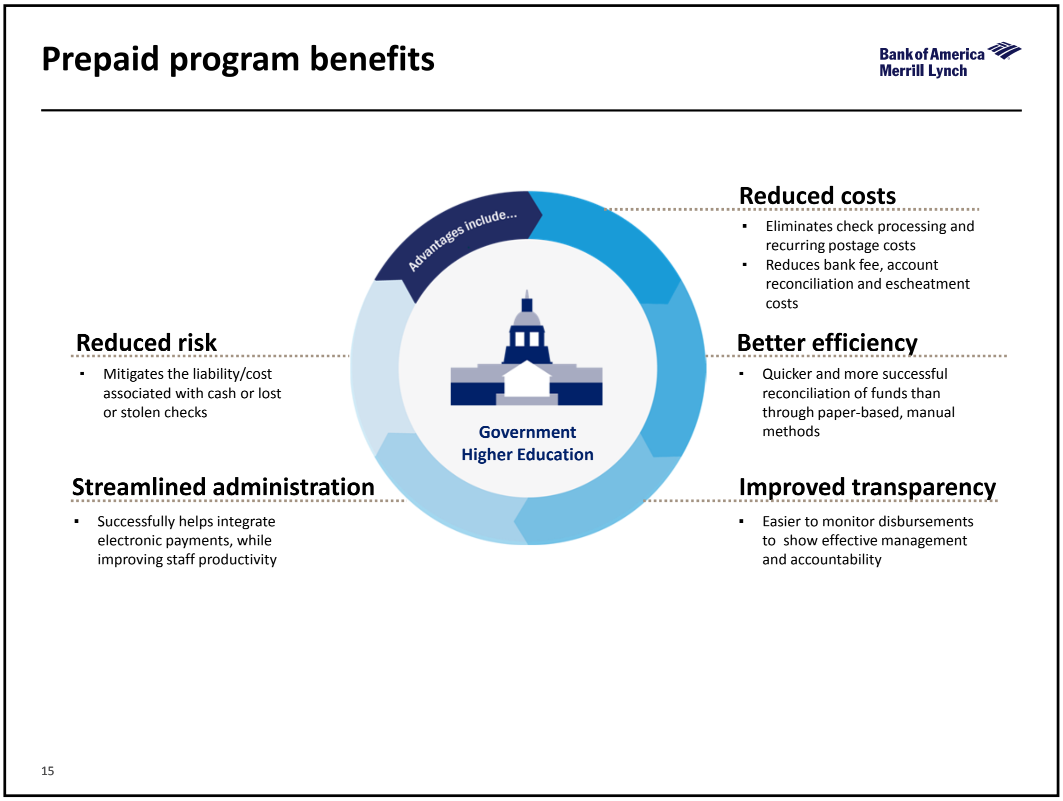
Outstanding client service

Bank of America Merrill Lynch corporate and commercial banking call centers recognized
J.D. Power and Associates, 2013

Fastest growing issuer

Amongst the top 5 prepaid card issuers with a 45% purchase Volume growth rate in 2012
July 2013, Nilson Report

14



Prepaid program benefits

Bank of America Merrill Lynch

Advantages include…

Government Higher Education

Reduced costs

- Eliminates check processing and recurring postage costs
- Reduces bank fee, account reconciliation and escheatment costs

Reduced risk

- Mitigates the liability/cost associated with cash or lost or stolen checks

Better efficiency

- Quicker and more successful reconciliation of funds than through paper-based, manual methods

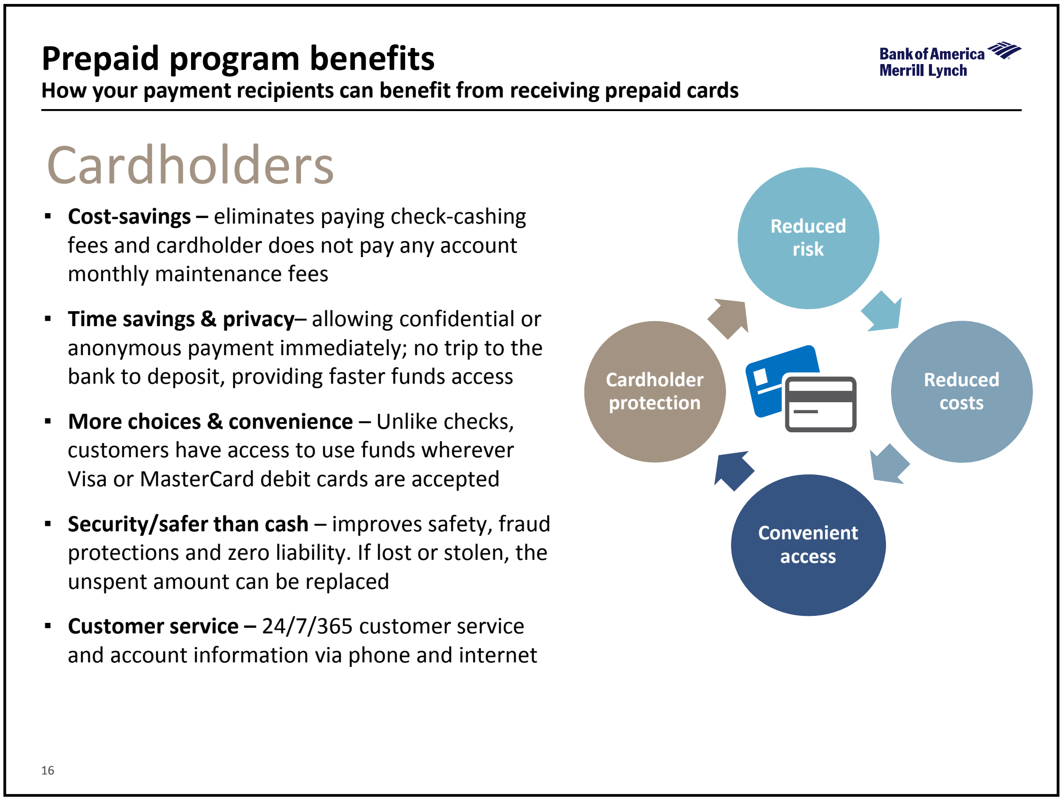
Streamlined administration

- Successfully helps integrate electronic payments, while improving staff productivity

Improved transparency

- Easier to monitor disbursements to show effective management and accountability

15



Prepaid program benefits

How your payment recipients can benefit from receiving prepaid cards

Bank of America Merrill Lynch

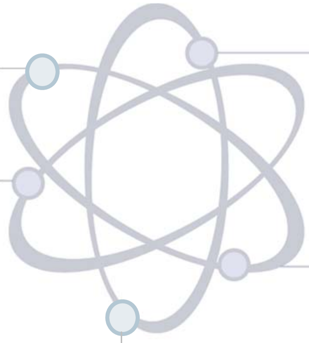
Cardholders

- **Cost-savings –** eliminates paying check-cashing fees and cardholder does not pay any account monthly maintenance fees
- **Time savings & privacy**– allowing confidential or anonymous payment immediately; no trip to the bank to deposit, providing faster funds access
- **More choices & convenience** – Unlike checks, customers have access to use funds wherever Visa or MasterCard debit cards are accepted
- **Security/safer than cash** – improves safety, fraud protections and zero liability. If lost or stolen, the unspent amount can be replaced
- **Customer service –** 24/7/365 customer service and account information via phone and internet

16

Key prepaid program features

Bank of America Merrill Lynch



24/7 support for your cardholders – Customer service is available through an online website, toll-free telephone access to an IVR of live agent call center

Dedicated client support– support including account management, implementation and client support hot line

Flexible product structures – Multiple product design and structure options, including ATM access.

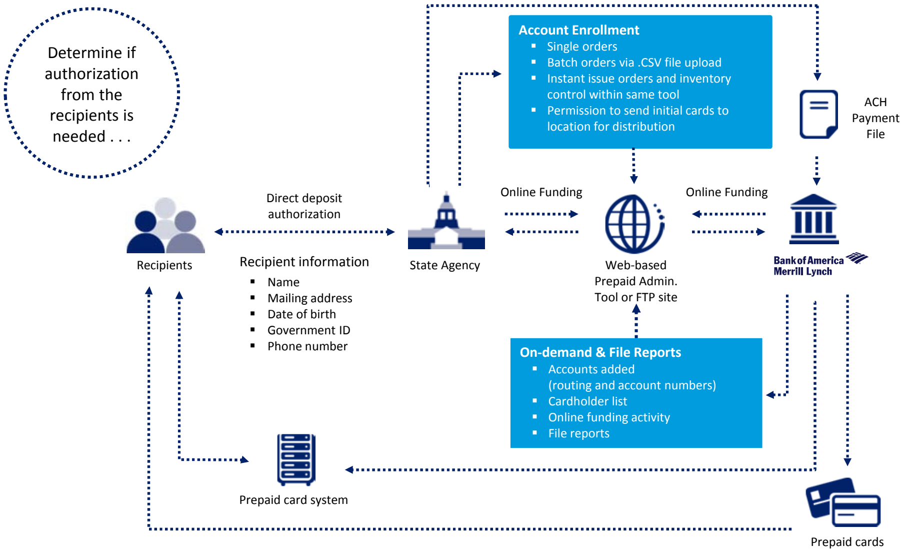
Easy to implement – You are assigned an implementation project manager to provide complete support as you design and launch your program

Easy to administer – Secure web-based tools to manage your program and access reporting

17

Account enrollment and funding process

Bank of America Merrill Lynch



Determine if authorization from the recipients is needed . . .

Account Enrollment

- Single orders
- Batch orders via .CSV file upload
- Instant issue orders and inventory control within same tool
- Permission to send initial cards to location for distribution

ACH Payment File
Direct deposit authorization
Online Funding
Online Funding
Recipients
State Agency
Web-based Prepaid Admin. Tool or FTP site
Bank of America Merrill Lynch
Prepaid card system
Prepaid cards

Recipient information

- Name
- Mailing address
- Date of birth
- Government ID
- Phone number

On-demand & File Reports

- Accounts added (routing and account numbers)
- Cardholder list
- Online funding activity
- File reports

18

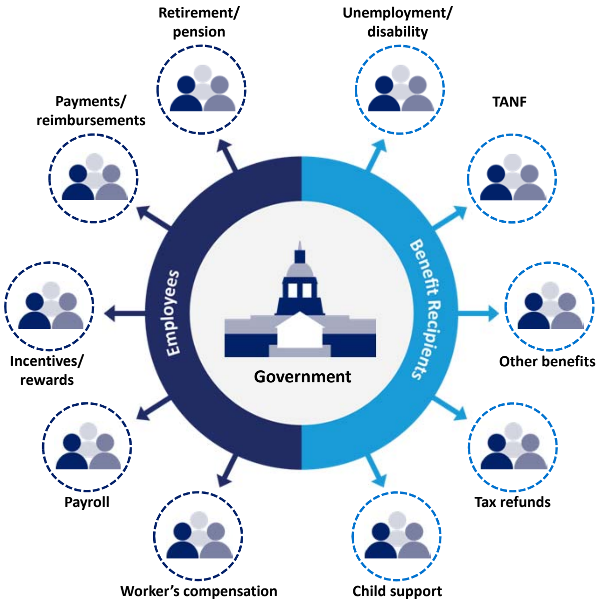
Prepaid Cards for Government

Government

Bank of America
Merrill Lynch

Multiple disbursement types

Bank of America
Merrill Lynch

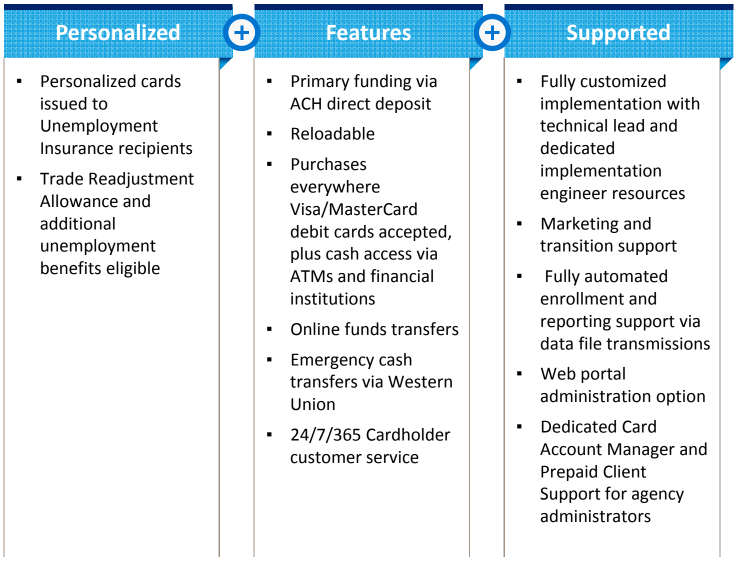


20

Use case: Unemployment insurance benefits

Recurring payments through prepaid cards

Bank of America Merrill Lynch



Personalized

- Personalized cards issued to Unemployment Insurance recipients
- Trade Readjustment Allowance and additional unemployment benefits eligible

+

Features

- Primary funding via ACH direct deposit
- Reloadable
- Purchases everywhere Visa/MasterCard debit cards accepted, plus cash access via ATMs and financial institutions
- Online funds transfers
- Emergency cash transfers via Western Union
- 24/7/365 Cardholder customer service

+

Supported

- Fully customized implementation with technical lead and dedicated implementation engineer resources
- Marketing and transition support
- Fully automated enrollment and reporting support via data file transmissions
- Web portal administration option
- Dedicated Card Account Manager and Prepaid Client Support for agency administrators

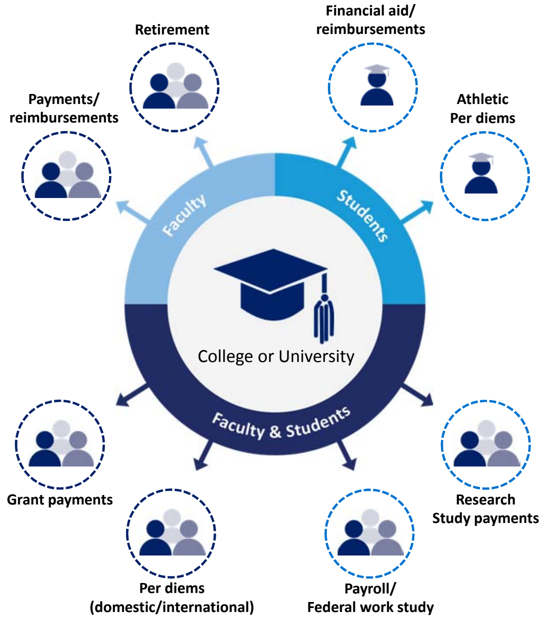
21

Prepaid Cards for Higher Education

Bank of America Merrill Lynch

Higher education payments – one of many disbursements

Bank of America Merrill Lynch



23

Use case: Research study payments

Immediate payment to participants through prepaid cards

Bank of America Merrill Lynch

Product models

Anonymous +

- Instant issuance of card to study participants
- Single load up to $1,000
- Cash access restricted

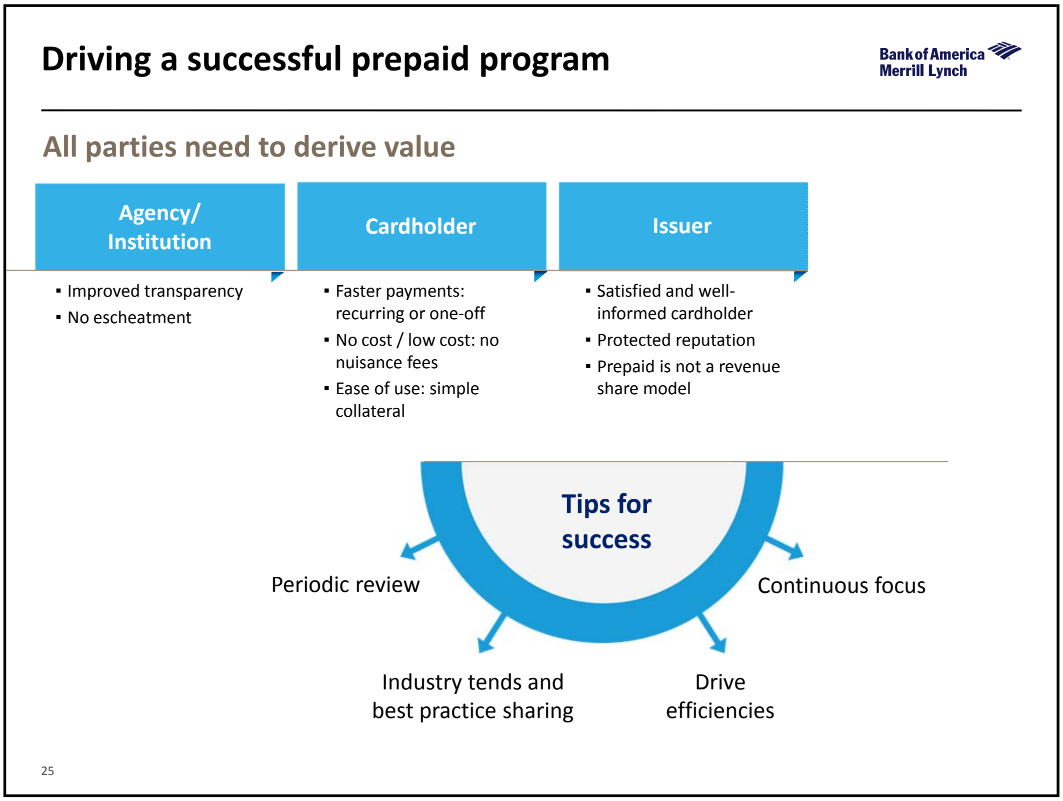
Registered +

- Instant issuance of card to study participants (non-personalized)
- Reloadable up to $5,000
- Cash access allowed
- Cardholder website

Supported

- Study-level reporting
- Web portal with security functions to segregate funding and enrollment
- Card inventory management system
- Logo customized card, if desired

24



Driving a successful prepaid program

Bank of America Merrill Lynch

All parties need to derive value

Agency/ Institution	Cardholder	Issuer
▪ Improved transparency ▪ No escheatment	▪ Faster payments: recurring or one-off ▪ No cost / low cost: no nuisance fees ▪ Ease of use: simple collateral	▪ Satisfied and well-informed cardholder ▪ Protected reputation ▪ Prepaid is not a revenue share model

Tips for success

- Periodic review
- Industry tends and best practice sharing
- Drive efficiencies
- Continuous focus

25

Questions & Open Discussion

Bank of America Merrill Lynch

Appendices

Our prepaid card credentials

Bank of America
Merrill Lynch

Our commitment

Bank of America
Merrill Lynch

Why Bank of America Merrill Lynch

- A leader in prepaid card solutions, with new programs in the government agency market
- Over 15 years experience providing prepaid card solutions to corporations, government agencies or higher education institutions, as well as individual cardholders
- Leading provider of debit card transactions with over 85 billion transactions processed annually based on 30 million cards issued
- Supports the largest unemployment and disability insurance prepaid card program in the U.S. (California Employment Development department—CA EDD)
- A leader in state tax refund prepaid card programs
- User friendly, web-enabled platform for managing programs
- 24/7 cardholder support in English and Spanish
- Account access at 16,300 ATMs coast to coast—with no ATM fees
- Prepaid card accounts are FDIC insured, with full Regulation E compliance

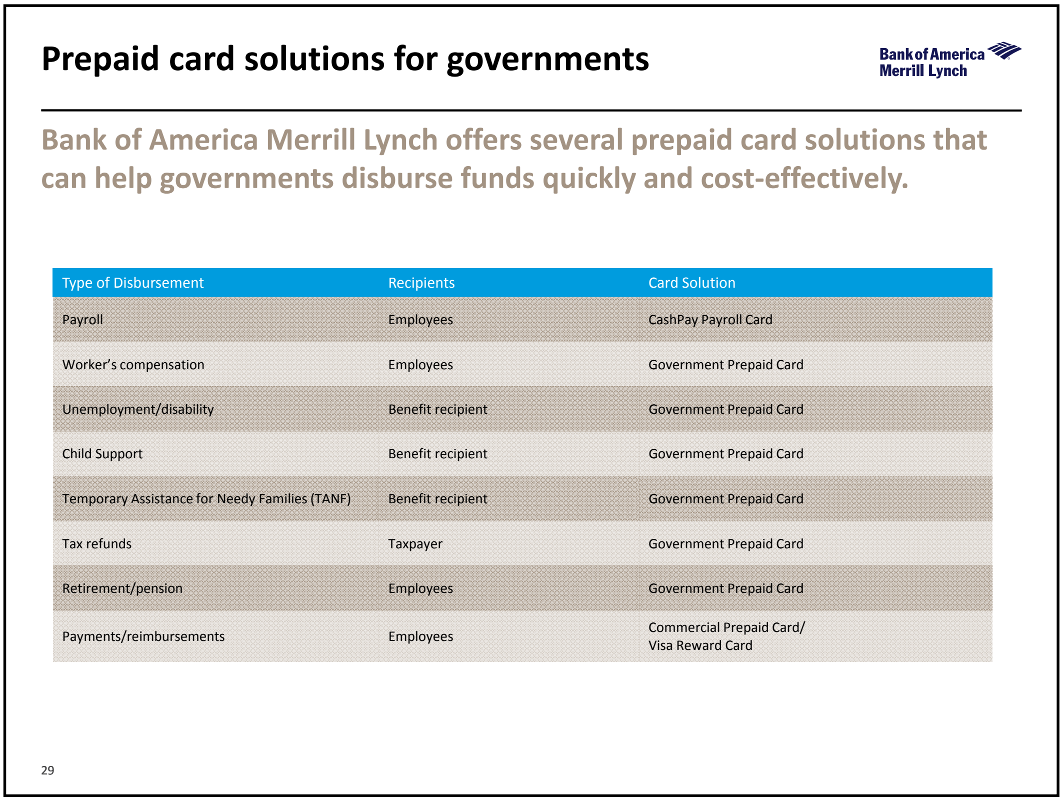
Case Study:
Success with the CA EDD

CA EDD is the largest [state agency prepaid card] program in the country.

The program is a major undertaking for the state. In 2009, EDD paid out $20.2 billion in unemployment insurance benefits, $4.3 billion in disability benefits and $462 million for paid family leave.

EDD believes going paperless will save $4 million in printing and postage costs once the payments are fully converted.

Source: The Orange County Register,
State disability pay goes plastic (January 10, 2011)

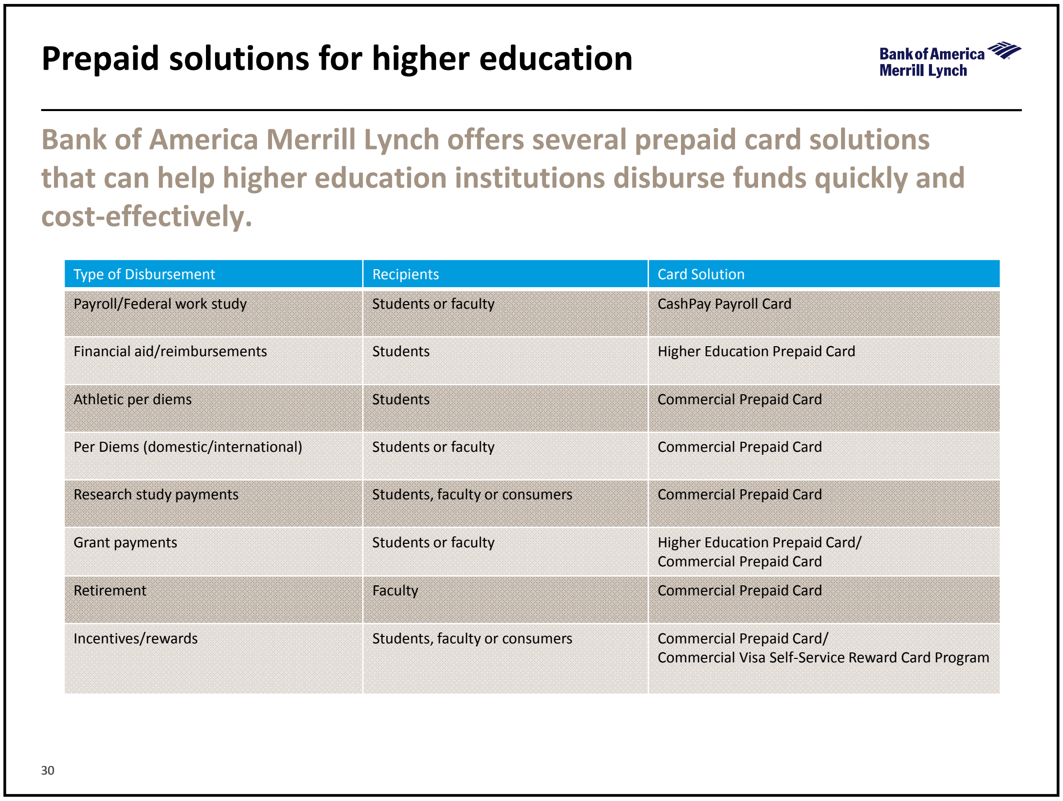


Prepaid card solutions for governments

Bank of America Merrill Lynch

Bank of America Merrill Lynch offers several prepaid card solutions that can help governments disburse funds quickly and cost-effectively.

Type of Disbursement	Recipients	Card Solution
Payroll	Employees	CashPay Payroll Card
Worker’s compensation	Employees	Government Prepaid Card
Unemployment/disability	Benefit recipient	Government Prepaid Card
Child Support	Benefit recipient	Government Prepaid Card
Temporary Assistance for Needy Families (TANF)	Benefit recipient	Government Prepaid Card
Tax refunds	Taxpayer	Government Prepaid Card
Retirement/pension	Employees	Government Prepaid Card
Payments/reimbursements	Employees	Commercial Prepaid Card/ Visa Reward Card

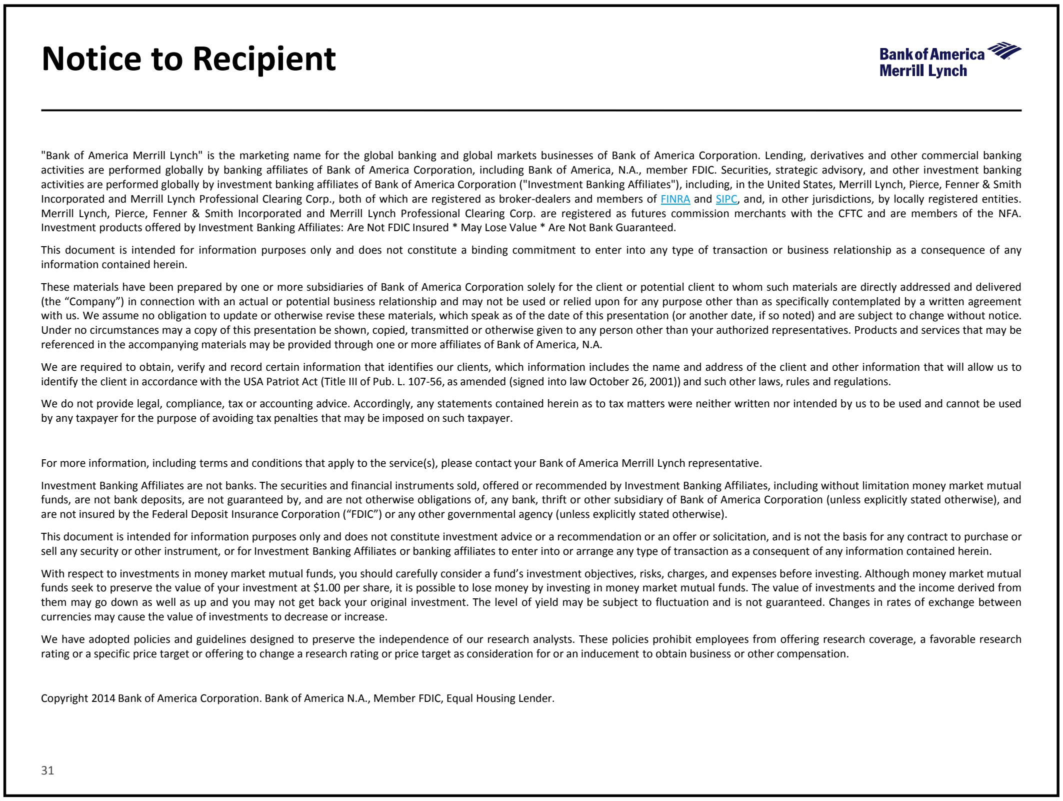


Prepaid solutions for higher education

Bank of America Merrill Lynch

Bank of America Merrill Lynch offers several prepaid card solutions that can help higher education institutions disburse funds quickly and cost-effectively.

Type of Disbursement	Recipients	Card Solution
Payroll/Federal work study	Students or faculty	CashPay Payroll Card
Financial aid/reimbursements	Students	Higher Education Prepaid Card
Athletic per diems	Students	Commercial Prepaid Card
Per Diems (domestic/international)	Students or faculty	Commercial Prepaid Card
Research study payments	Students, faculty or consumers	Commercial Prepaid Card
Grant payments	Students or faculty	Higher Education Prepaid Card/ Commercial Prepaid Card
Retirement	Faculty	Commercial Prepaid Card
Incentives/rewards	Students, faculty or consumers	Commercial Prepaid Card/ Commercial Visa Self-Service Reward Card Program



Notice to Recipient

"Bank of America Merrill Lynch" is the marketing name for the global banking and global markets businesses of Bank of America Corporation. Lending, derivatives and other commercial banking activities are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., member FDIC. Securities, strategic advisory, and other investment banking activities are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp., both of which are registered as broker-dealers and members of FINRA and SIPC, and, in other jurisdictions, by locally registered entities. Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA. Investment products offered by Investment Banking Affiliates: Are Not FDIC Insured * May Lose Value * Are Not Bank Guaranteed.

This document is intended for information purposes only and does not constitute a binding commitment to enter into any type of transaction or business relationship as a consequence of any information contained herein.

These materials have been prepared by one or more subsidiaries of Bank of America Corporation solely for the client or potential client to whom such materials are directly addressed and delivered (the “Company”) in connection with an actual or potential business relationship and may not be used or relied upon for any purpose other than as specifically contemplated by a written agreement with us. We assume no obligation to update or otherwise revise these materials, which speak as of the date of this presentation (or another date, if so noted) and are subject to change without notice. Under no circumstances may a copy of this presentation be shown, copied, transmitted or otherwise given to any person other than your authorized representatives. Products and services that may be referenced in the accompanying materials may be provided through one or more affiliates of Bank of America, N.A.

We are required to obtain, verify and record certain information that identifies our clients, which information includes the name and address of the client and other information that will allow us to identify the client in accordance with the USA Patriot Act (Title III of Pub. L. 107-56, as amended (signed into law October 26, 2001)) and such other laws, rules and regulations.

We do not provide legal, compliance, tax or accounting advice. Accordingly, any statements contained herein as to tax matters were neither written nor intended by us to be used and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed on such taxpayer.

For more information, including terms and conditions that apply to the service(s), please contact your Bank of America Merrill Lynch representative.

Investment Banking Affiliates are not banks. The securities and financial instruments sold, offered or recommended by Investment Banking Affiliates, including without limitation money market mutual funds, are not bank deposits, are not guaranteed by, and are not otherwise obligations of, any bank, thrift or other subsidiary of Bank of America Corporation (unless explicitly stated otherwise), and are not insured by the Federal Deposit Insurance Corporation (“FDIC”) or any other governmental agency (unless explicitly stated otherwise).

This document is intended for information purposes only and does not constitute investment advice or a recommendation or an offer or solicitation, and is not the basis for any contract to purchase or sell any security or other instrument, or for Investment Banking Affiliates or banking affiliates to enter into or arrange any type of transaction as a consequent of any information contained herein.

With respect to investments in money market mutual funds, you should carefully consider a fund’s investment objectives, risks, charges, and expenses before investing. Although money market mutual funds seek to preserve the value of your investment at $1.00 per share, it is possible to lose money by investing in money market mutual funds. The value of investments and the income derived from them may go down as well as up and you may not get back your original investment. The level of yield may be subject to fluctuation and is not guaranteed. Changes in rates of exchange between currencies may cause the value of investments to decrease or increase.

We have adopted policies and guidelines designed to preserve the independence of our research analysts. These policies prohibit employees from offering research coverage, a favorable research rating or a specific price target or offering to change a research rating or price target as consideration for or an inducement to obtain business or other compensation.

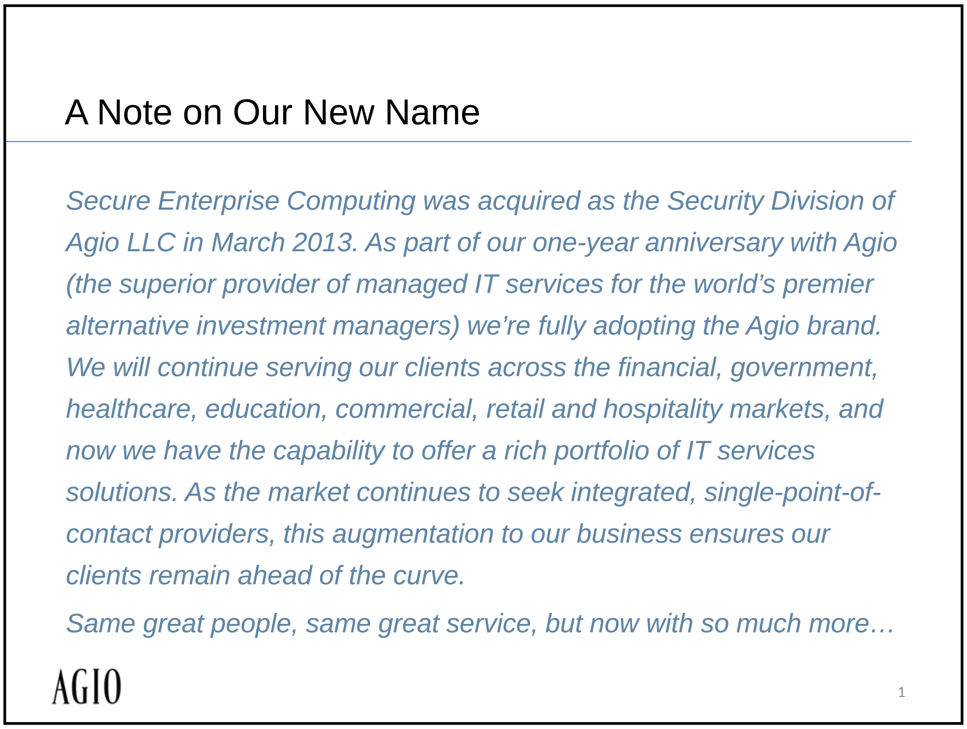
PCI DSS Security Awareness Training

North Carolina Office of the State Controller – Technology Meeting

April 30, 2014

AGIO

agio.com



A Note on Our New Name

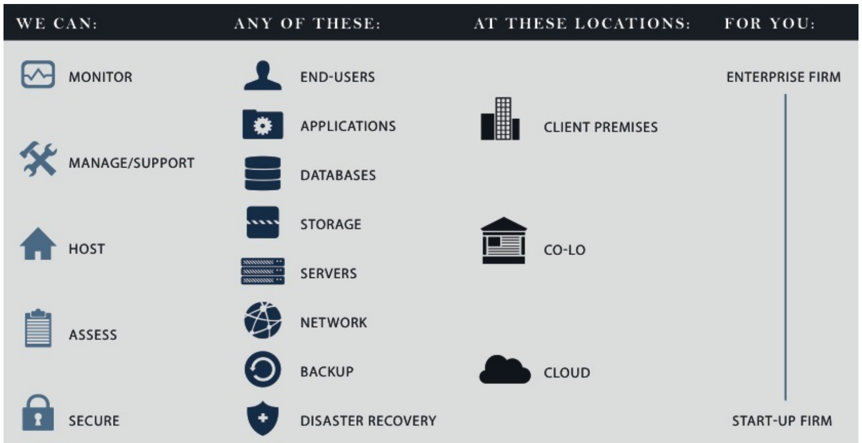
Secure Enterprise Computing was acquired as the Security Division of Agio LLC in March 2013. As part of our one-year anniversary with Agio (the superior provider of managed IT services for the world's premier alternative investment managers) we're fully adopting the Agio brand. We will continue serving our clients across the financial, government, healthcare, education, commercial, retail and hospitality markets, and now we have the capability to offer a rich portfolio of IT services solutions. As the market continues to seek integrated, single-point-of-contact providers, this augmentation to our business ensures our clients remain ahead of the curve.

Same great people, same great service, but now with so much more…

AGIO

1

Agio - What We Do



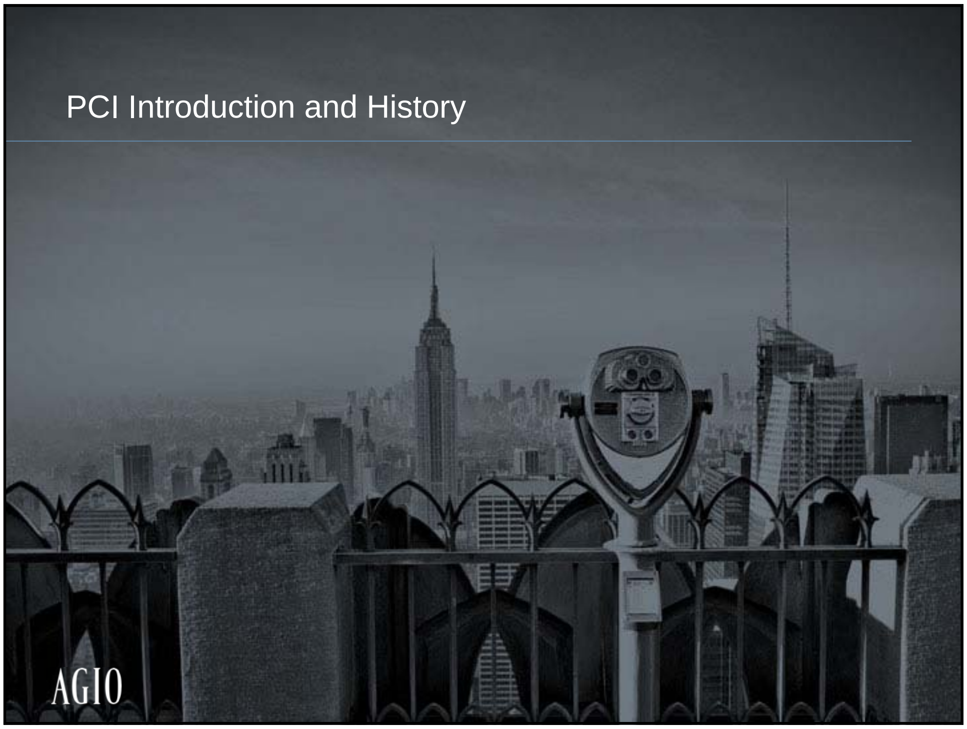
WE CAN:	ANY OF THESE:	AT THESE LOCATIONS:	FOR YOU:
MONITOR	END-USERS		ENTERPRISE FIRM
	APPLICATIONS	CLIENT PREMISES	
MANAGE/SUPPORT	DATABASES		
	STORAGE		
HOST	SERVERS	CO-LO	
ASSESS	NETWORK		
	BACKUP	CLOUD	
SECURE	DISASTER RECOVERY		START-UP FIRM

AGIO

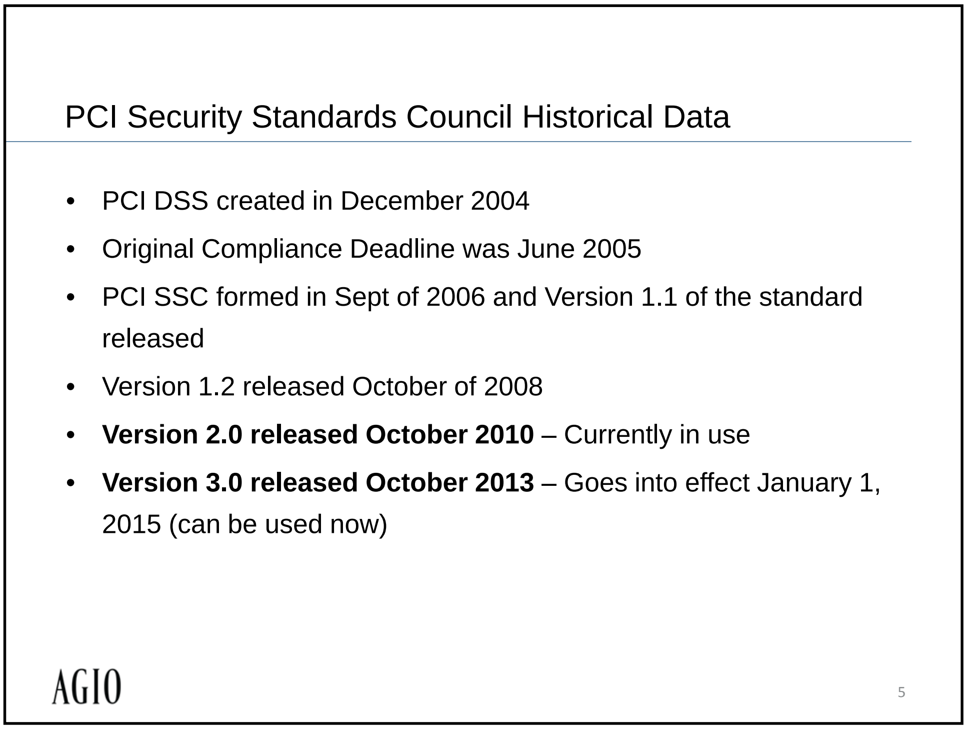
Our Security Credentials

- 20+ years of continuous service as IT Security Consultants and Security VAR
- 15+ years conducting compliance-based assessments
- PCI Qualified Security Assessor (QSA) since 2009
- PCI Approved Scanning Vendor (ASV) since 2006
- HITRUST (HIPAA/HITECH) Certified Practitioners
- 1 of 9 companies pre-approved by State of NC to conduct assessments for state agencies and higher education
- Consultants hold many certifications including CISSP, SANS, etc. and have on average 15 years of experience

AGIO

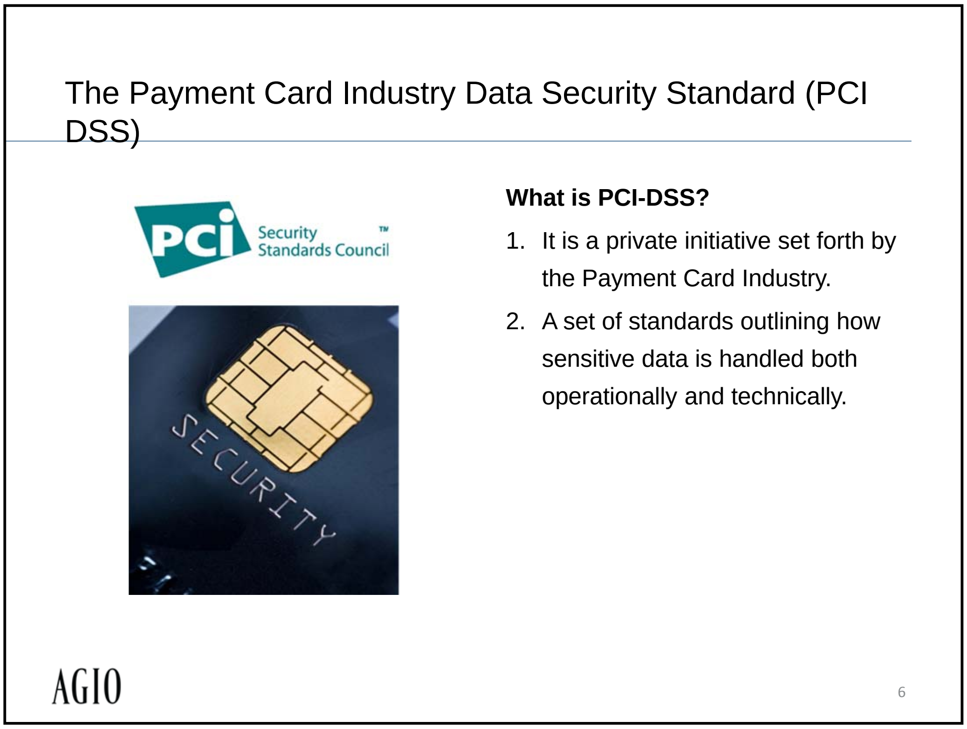


PCI Introduction and History



PCI Security Standards Council Historical Data

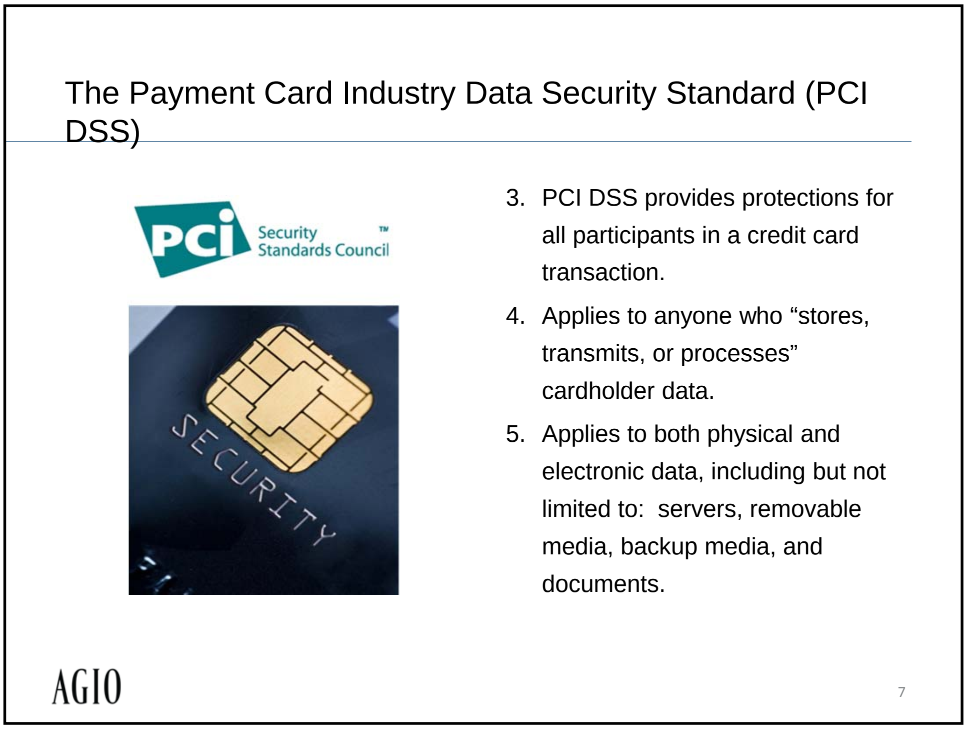
- PCI DSS created in December 2004
- Original Compliance Deadline was June 2005
- PCI SSC formed in Sept of 2006 and Version 1.1 of the standard released
- Version 1.2 released October of 2008
- **Version 2.0 released October 2010** – Currently in use
- **Version 3.0 released October 2013** – Goes into effect January 1, 2015 (can be used now)



The Payment Card Industry Data Security Standard (PCI DSS)

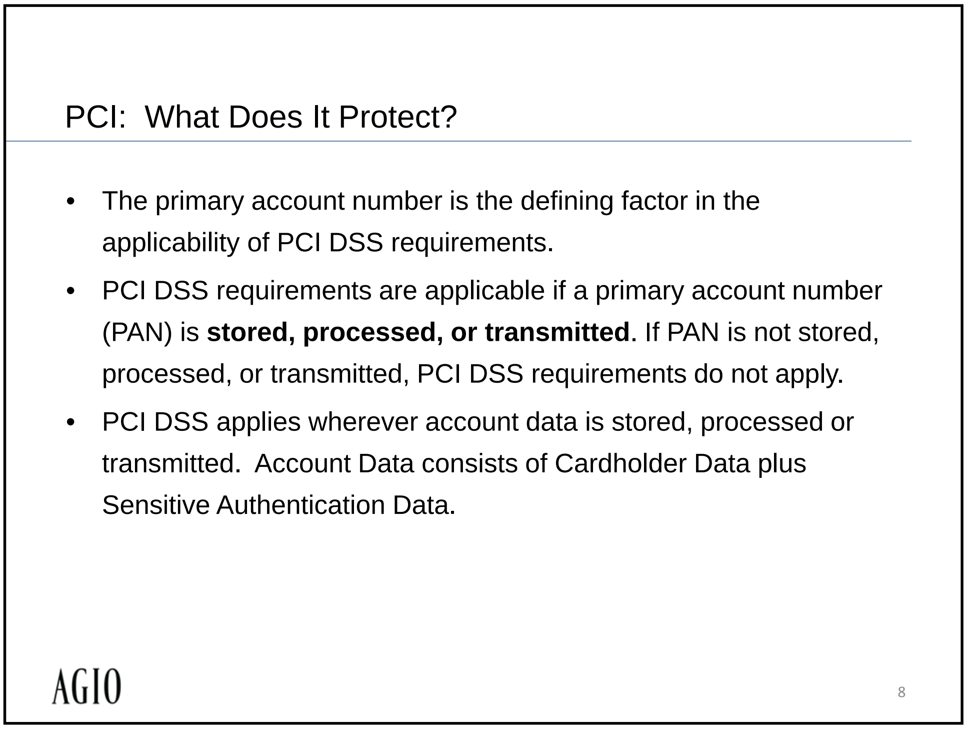
What is PCI-DSS?

1. It is a private initiative set forth by the Payment Card Industry.
2. A set of standards outlining how sensitive data is handled both operationally and technically.



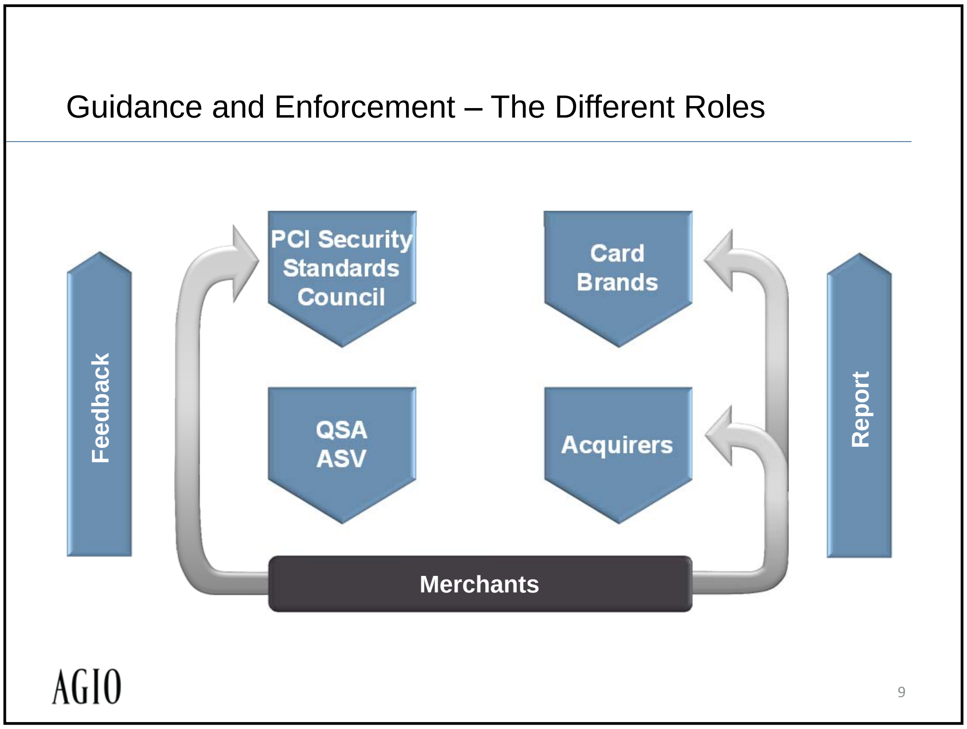
The Payment Card Industry Data Security Standard (PCI DSS)

3. PCI DSS provides protections for all participants in a credit card transaction.
4. Applies to anyone who “stores, transmits, or processes” cardholder data.
5. Applies to both physical and electronic data, including but not limited to: servers, removable media, backup media, and documents.



PCI: What Does It Protect?

- The primary account number is the defining factor in the applicability of PCI DSS requirements.
- PCI DSS requirements are applicable if a primary account number (PAN) is **stored, processed, or transmitted**. If PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.
- PCI DSS applies wherever account data is stored, processed or transmitted. Account Data consists of Cardholder Data plus Sensitive Authentication Data.



Guidance and Enforcement – The Different Roles

Feedback

PCI Security Standards Council

Card Brands

QSA ASV

Acquirers

Report

Merchants

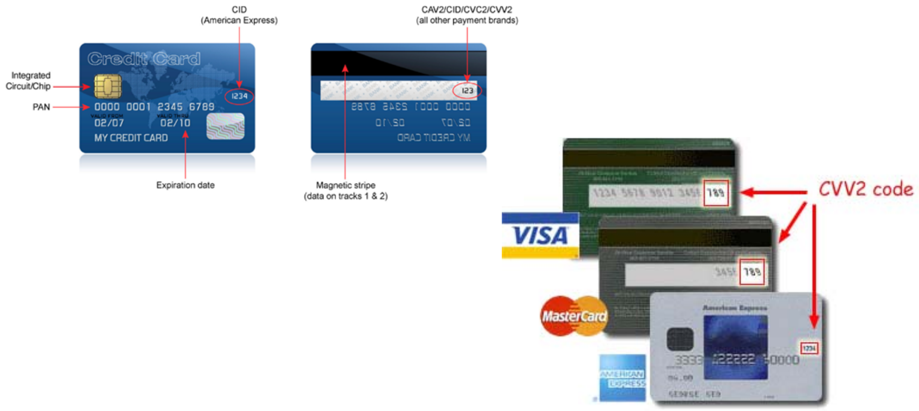
PCI: What Can Be Stored and How?

	Data Element	Storage Permitted ?	Render Stored Account Data Unreadable
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication Data	Full Magnetic Stripe Data	No	Cannot store after authorization
	CAV2/CVC2/CVV2/CID	No	Cannot store after authorization
	PIN/PIN Block	No	Cannot store after authorization

AGIO

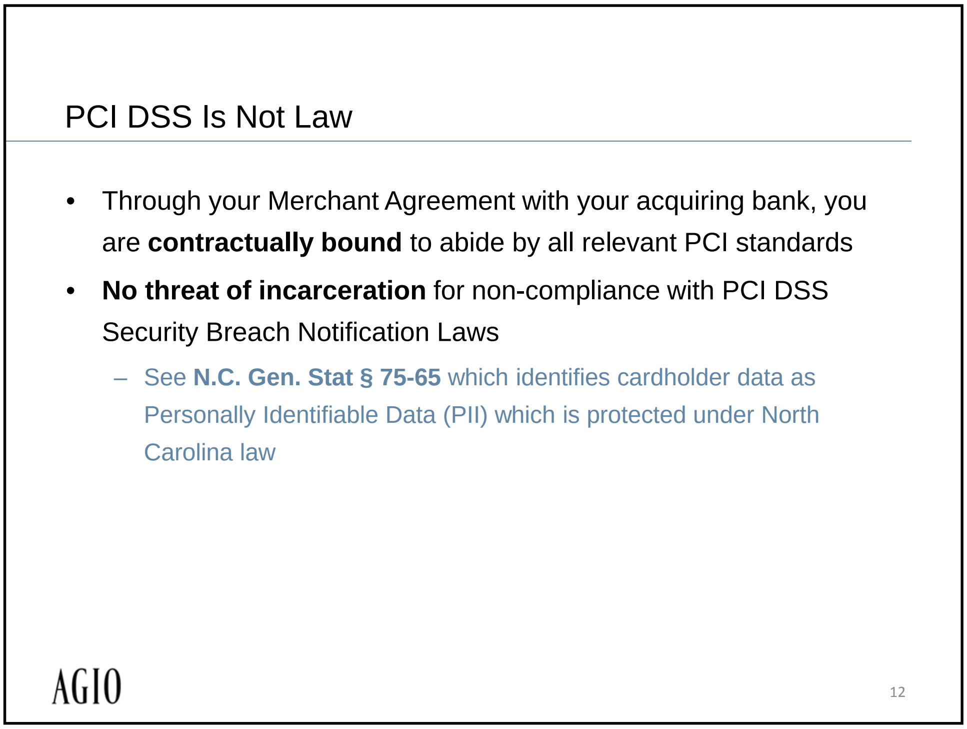
10

Cardholder Data



AGIO

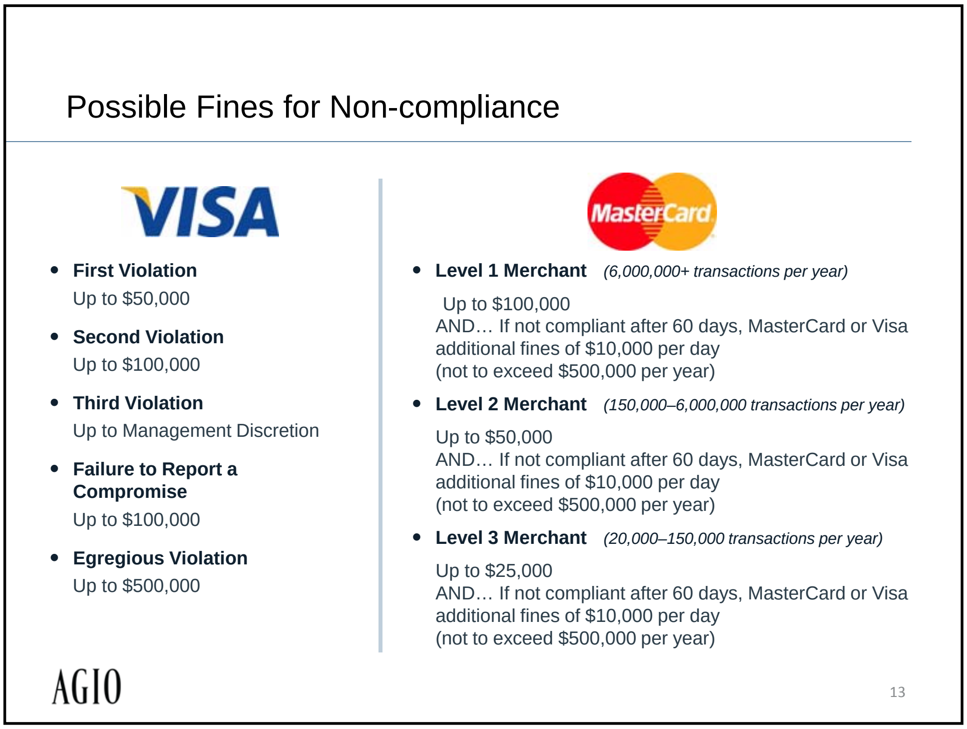
11



PCI DSS Is Not Law

- Through your Merchant Agreement with your acquiring bank, you are **contractually bound** to abide by all relevant PCI standards
- **No threat of incarceration** for non-compliance with PCI DSS Security Breach Notification Laws
  - See **N.C. Gen. Stat § 75-65** which identifies cardholder data as Personally Identifiable Data (PII) which is protected under North Carolina law

AGIO



Possible Fines for Non-compliance

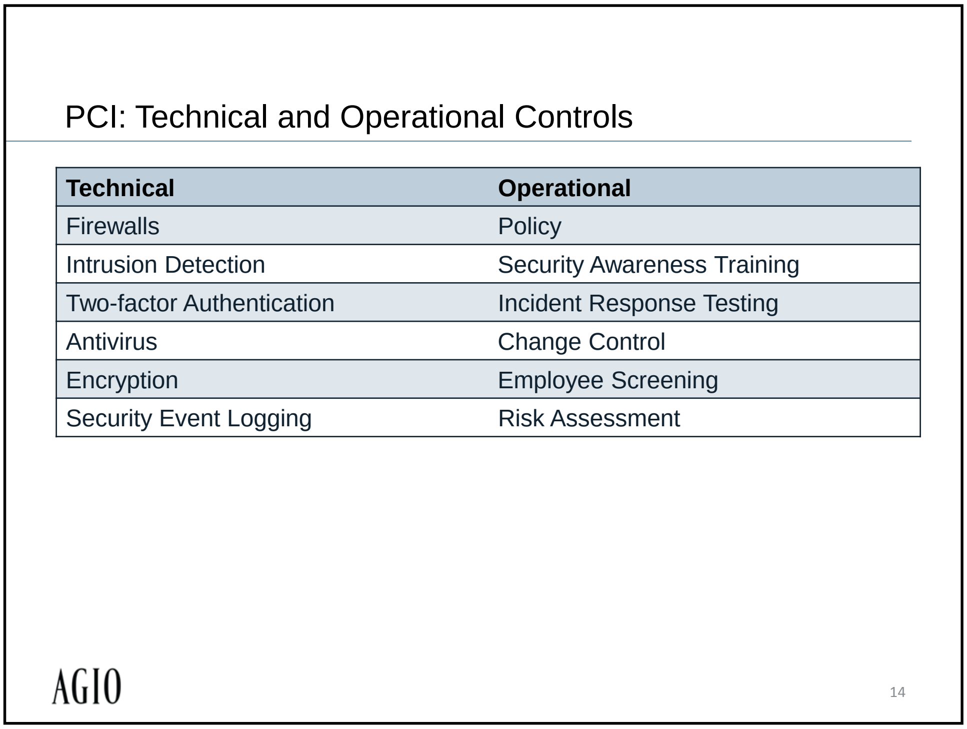
VISA

- **First Violation**
  Up to $50,000
- **Second Violation**
  Up to $100,000
- **Third Violation**
  Up to Management Discretion
- **Failure to Report a Compromise**
  Up to $100,000
- **Egregious Violation**
  Up to $500,000

MasterCard

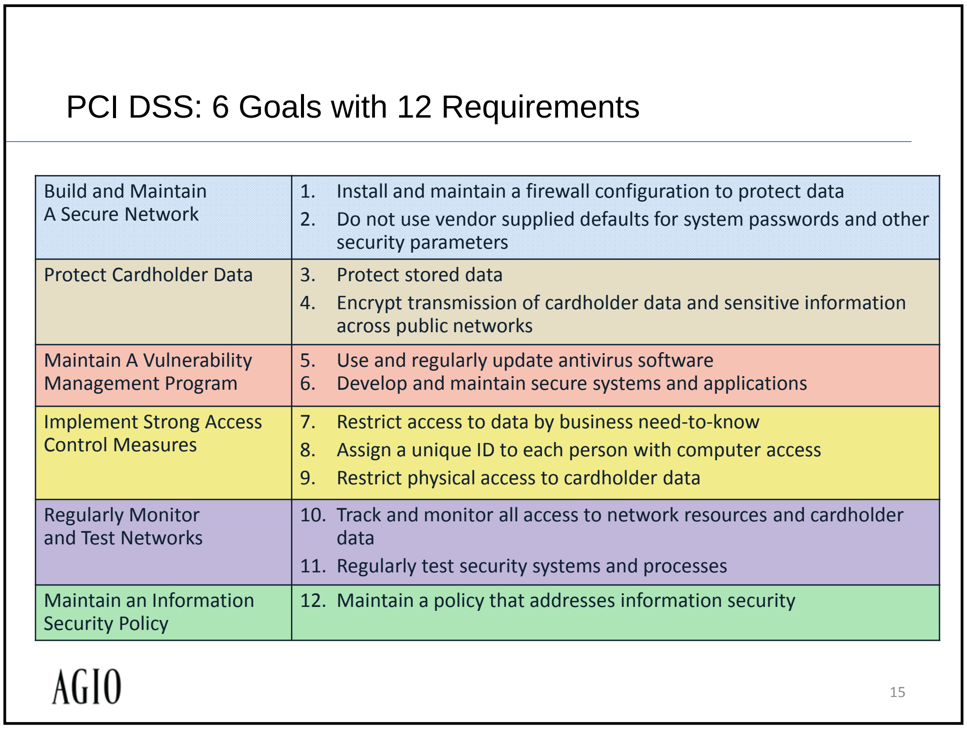
- **Level 1 Merchant** *(6,000,000+ transactions per year)*
  Up to $100,000
  AND… If not compliant after 60 days, MasterCard or Visa additional fines of $10,000 per day
  (not to exceed $500,000 per year)
- **Level 2 Merchant** *(150,000–6,000,000 transactions per year)*
  Up to $50,000
  AND… If not compliant after 60 days, MasterCard or Visa additional fines of $10,000 per day
  (not to exceed $500,000 per year)
- **Level 3 Merchant** *(20,000–150,000 transactions per year)*
  Up to $25,000
  AND… If not compliant after 60 days, MasterCard or Visa additional fines of $10,000 per day
  (not to exceed $500,000 per year)

AGIO



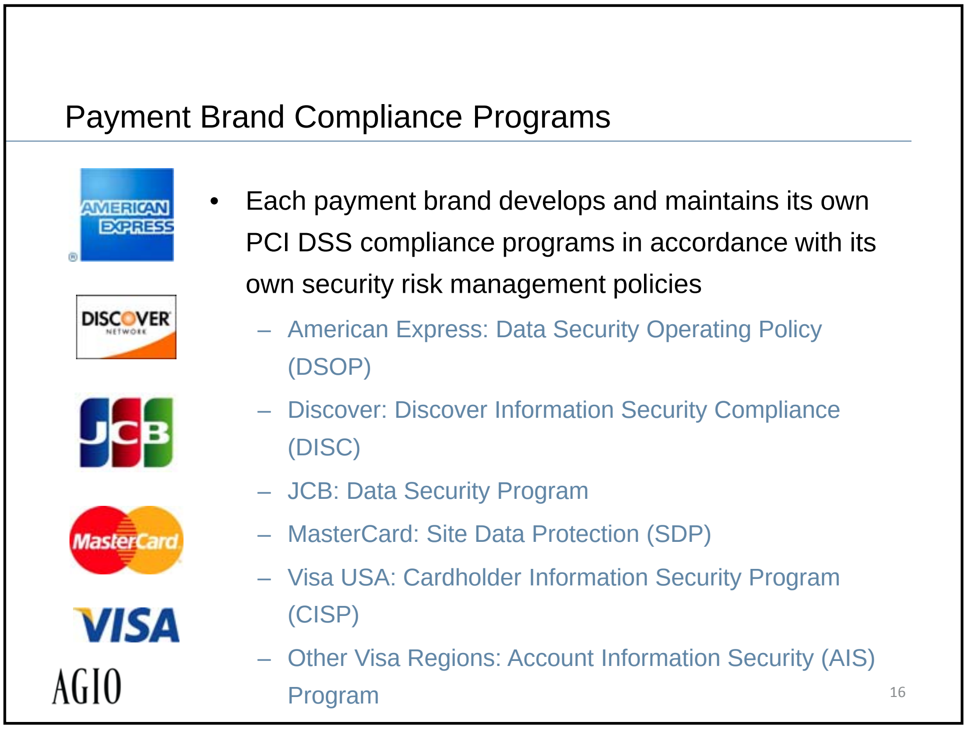
PCI: Technical and Operational Controls

Technical	Operational
Firewalls	Policy
Intrusion Detection	Security Awareness Training
Two-factor Authentication	Incident Response Testing
Antivirus	Change Control
Encryption	Employee Screening
Security Event Logging	Risk Assessment



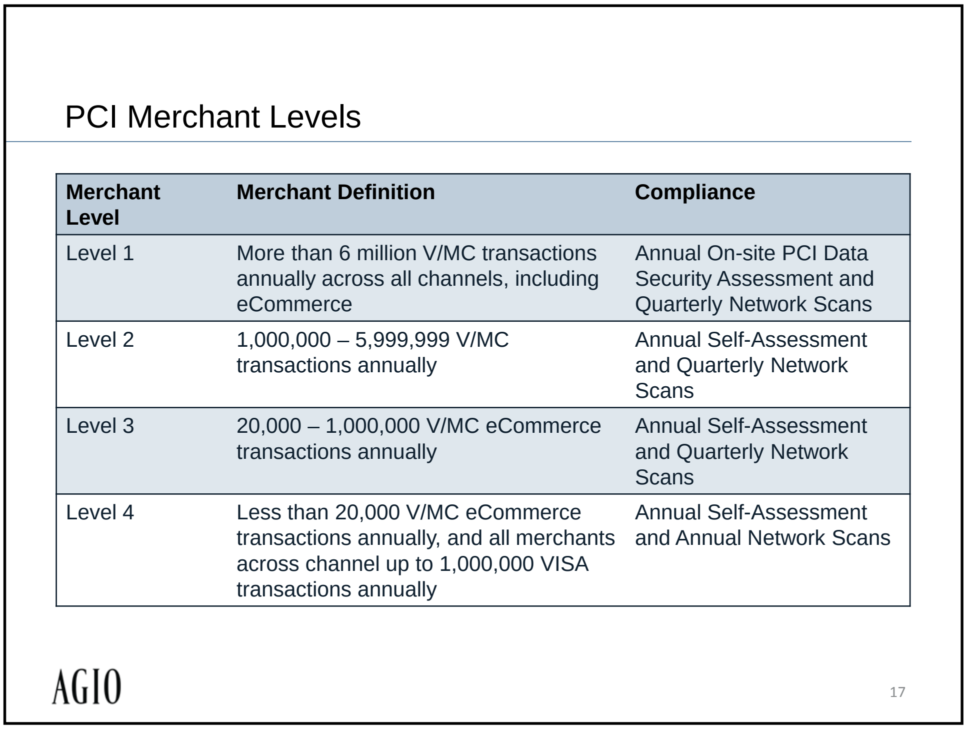
PCI DSS: 6 Goals with 12 Requirements

Build and Maintain A Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain A Vulnerability Management Program	5. Use and regularly update antivirus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security



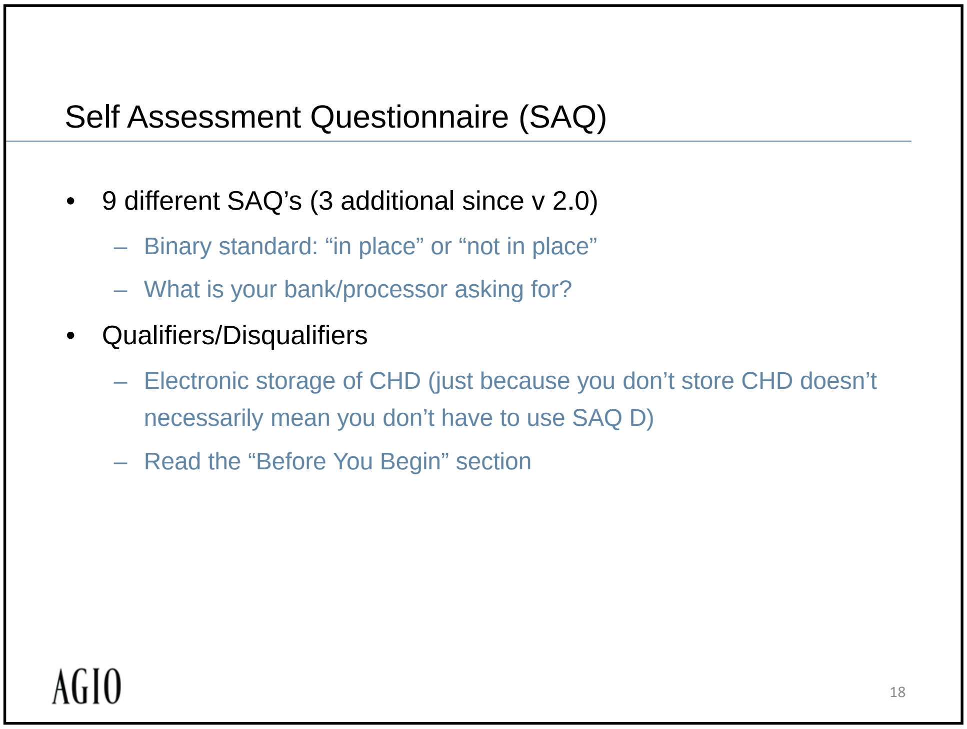
Payment Brand Compliance Programs

- Each payment brand develops and maintains its own PCI DSS compliance programs in accordance with its own security risk management policies
  - American Express: Data Security Operating Policy (DSOP)
  - Discover: Discover Information Security Compliance (DISC)
  - JCB: Data Security Program
  - MasterCard: Site Data Protection (SDP)
  - Visa USA: Cardholder Information Security Program (CISP)
  - Other Visa Regions: Account Information Security (AIS) Program



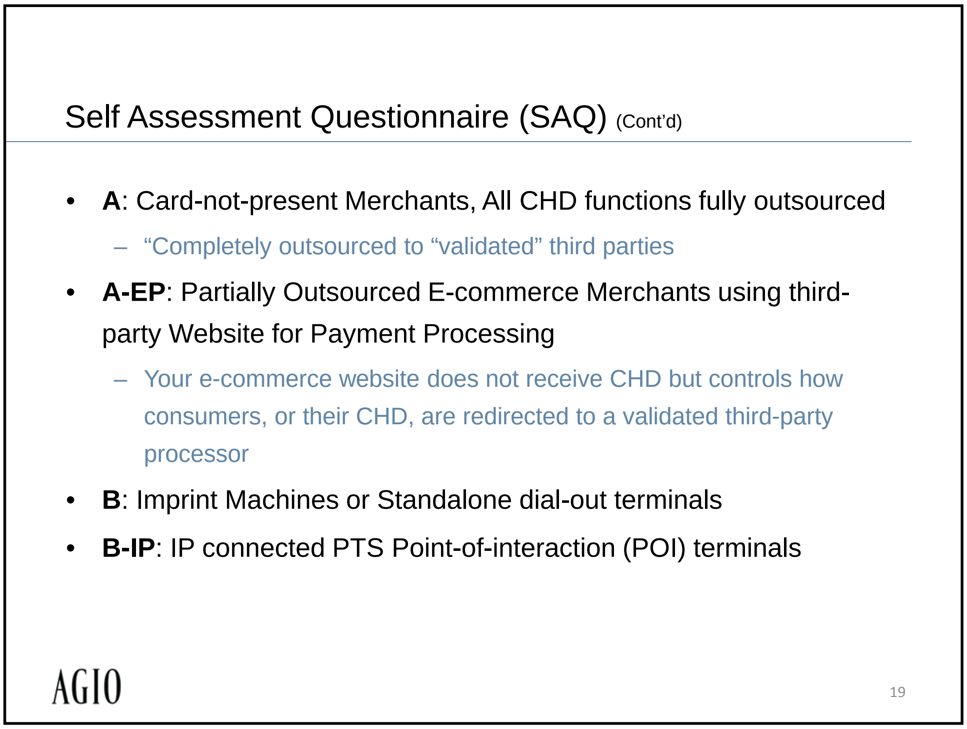
PCI Merchant Levels

Merchant Level	Merchant Definition	Compliance
Level 1	More than 6 million V/MC transactions annually across all channels, including eCommerce	Annual On-site PCI Data Security Assessment and Quarterly Network Scans
Level 2	1,000,000 – 5,999,999 V/MC transactions annually	Annual Self-Assessment and Quarterly Network Scans
Level 3	20,000 – 1,000,000 V/MC eCommerce transactions annually	Annual Self-Assessment and Quarterly Network Scans
Level 4	Less than 20,000 V/MC eCommerce transactions annually, and all merchants across channel up to 1,000,000 VISA transactions annually	Annual Self-Assessment and Annual Network Scans



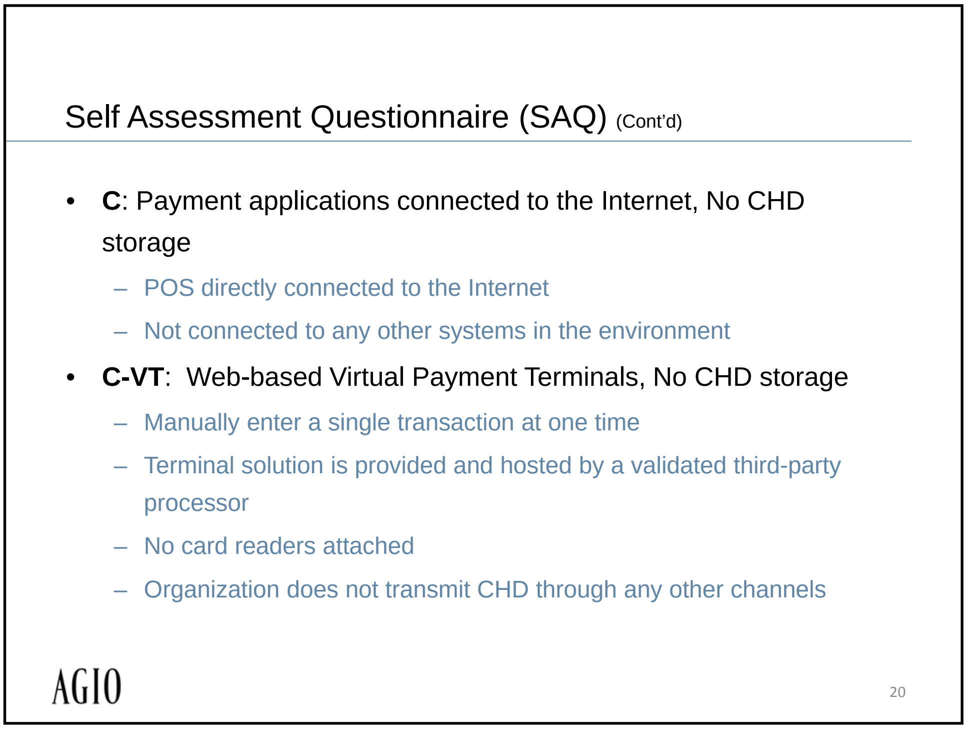
Self Assessment Questionnaire (SAQ)

- 9 different SAQ's (3 additional since v 2.0)
  - Binary standard: "in place" or "not in place"
  - What is your bank/processor asking for?
- Qualifiers/Disqualifiers
  - Electronic storage of CHD (just because you don't store CHD doesn't necessarily mean you don't have to use SAQ D)
  - Read the "Before You Begin" section



Self Assessment Questionnaire (SAQ) (Cont'd)

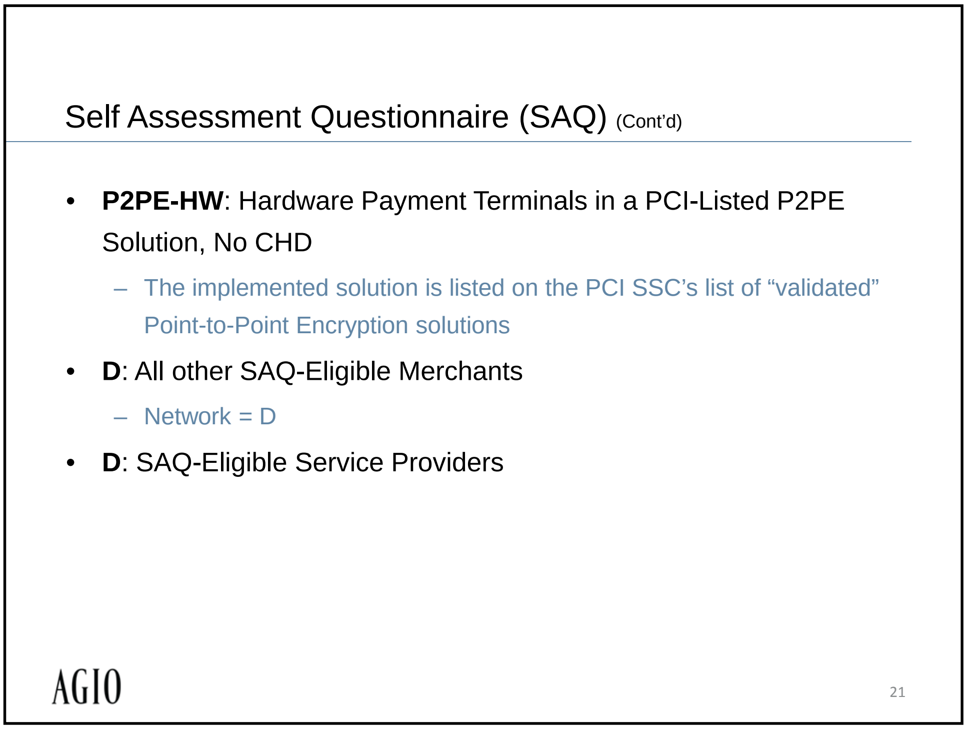
- **A**: Card-not-present Merchants, All CHD functions fully outsourced
  - "Completely outsourced to "validated" third parties
- **A-EP**: Partially Outsourced E-commerce Merchants using third-party Website for Payment Processing
  - Your e-commerce website does not receive CHD but controls how consumers, or their CHD, are redirected to a validated third-party processor
- **B**: Imprint Machines or Standalone dial-out terminals
- **B-IP**: IP connected PTS Point-of-interaction (POI) terminals



Self Assessment Questionnaire (SAQ) (Cont'd)

- **C**: Payment applications connected to the Internet, No CHD storage
  - POS directly connected to the Internet
  - Not connected to any other systems in the environment
- **C-VT**: Web-based Virtual Payment Terminals, No CHD storage
  - Manually enter a single transaction at one time
  - Terminal solution is provided and hosted by a validated third-party processor
  - No card readers attached
  - Organization does not transmit CHD through any other channels

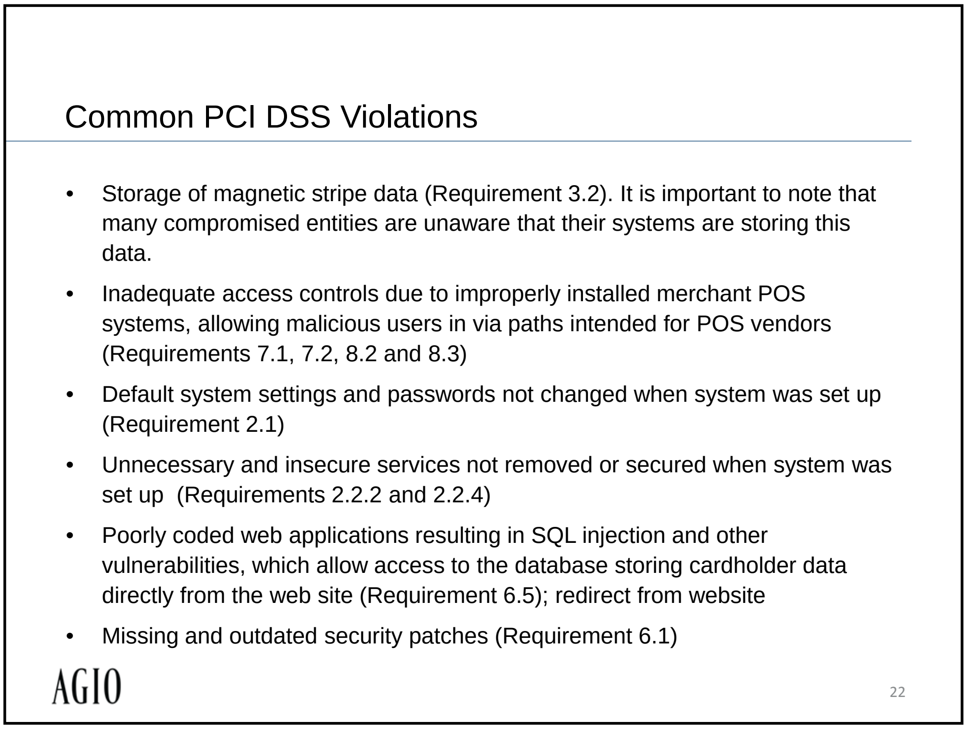
AGIO



Self Assessment Questionnaire (SAQ) (Cont'd)

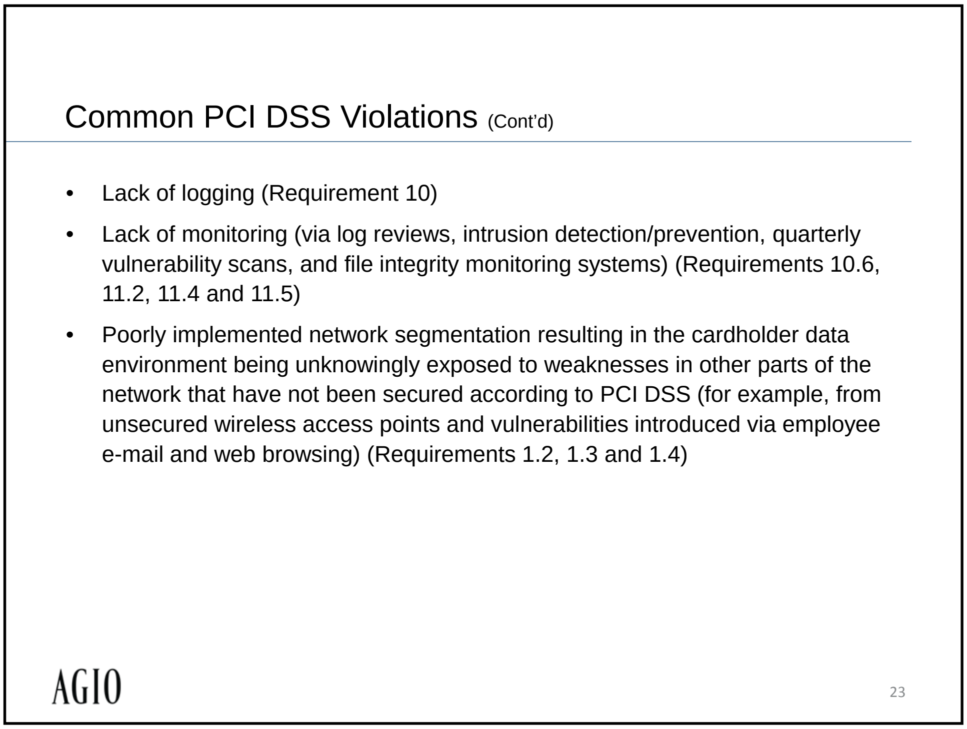
- **P2PE-HW**: Hardware Payment Terminals in a PCI-Listed P2PE Solution, No CHD
  - The implemented solution is listed on the PCI SSC's list of "validated" Point-to-Point Encryption solutions
- **D**: All other SAQ-Eligible Merchants
  - Network = D
- **D**: SAQ-Eligible Service Providers

AGIO



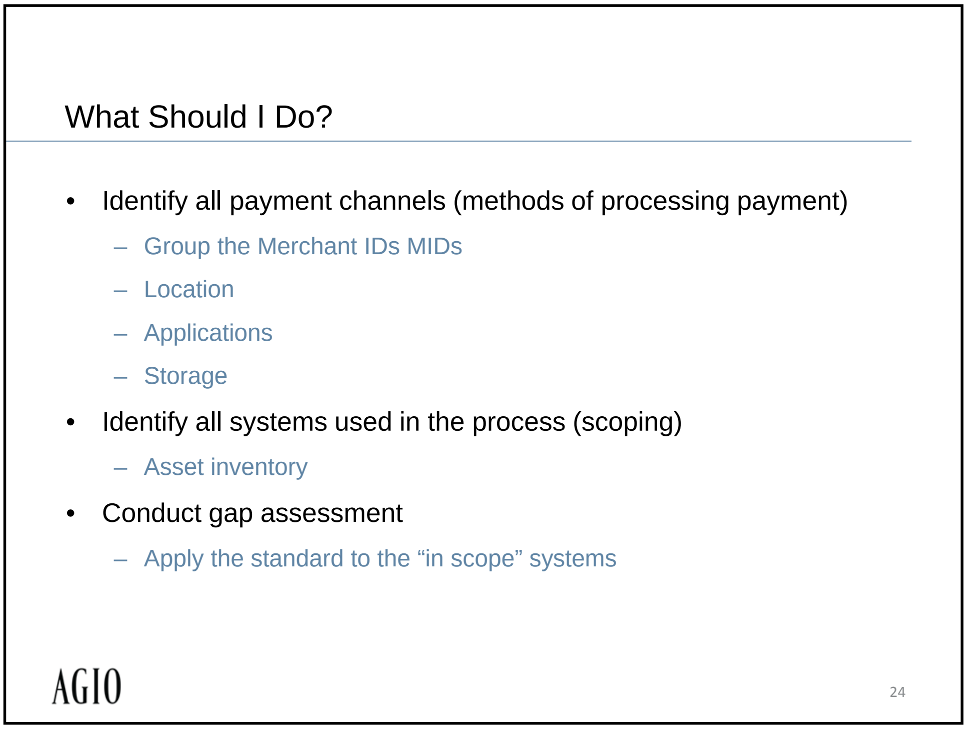
Common PCI DSS Violations

- Storage of magnetic stripe data (Requirement 3.2). It is important to note that many compromised entities are unaware that their systems are storing this data.
- Inadequate access controls due to improperly installed merchant POS systems, allowing malicious users in via paths intended for POS vendors (Requirements 7.1, 7.2, 8.2 and 8.3)
- Default system settings and passwords not changed when system was set up (Requirement 2.1)
- Unnecessary and insecure services not removed or secured when system was set up (Requirements 2.2.2 and 2.2.4)
- Poorly coded web applications resulting in SQL injection and other vulnerabilities, which allow access to the database storing cardholder data directly from the web site (Requirement 6.5); redirect from website
- Missing and outdated security patches (Requirement 6.1)



Common PCI DSS Violations (Cont'd)

- Lack of logging (Requirement 10)
- Lack of monitoring (via log reviews, intrusion detection/prevention, quarterly vulnerability scans, and file integrity monitoring systems) (Requirements 10.6, 11.2, 11.4 and 11.5)
- Poorly implemented network segmentation resulting in the cardholder data environment being unknowingly exposed to weaknesses in other parts of the network that have not been secured according to PCI DSS (for example, from unsecured wireless access points and vulnerabilities introduced via employee e-mail and web browsing) (Requirements 1.2, 1.3 and 1.4)

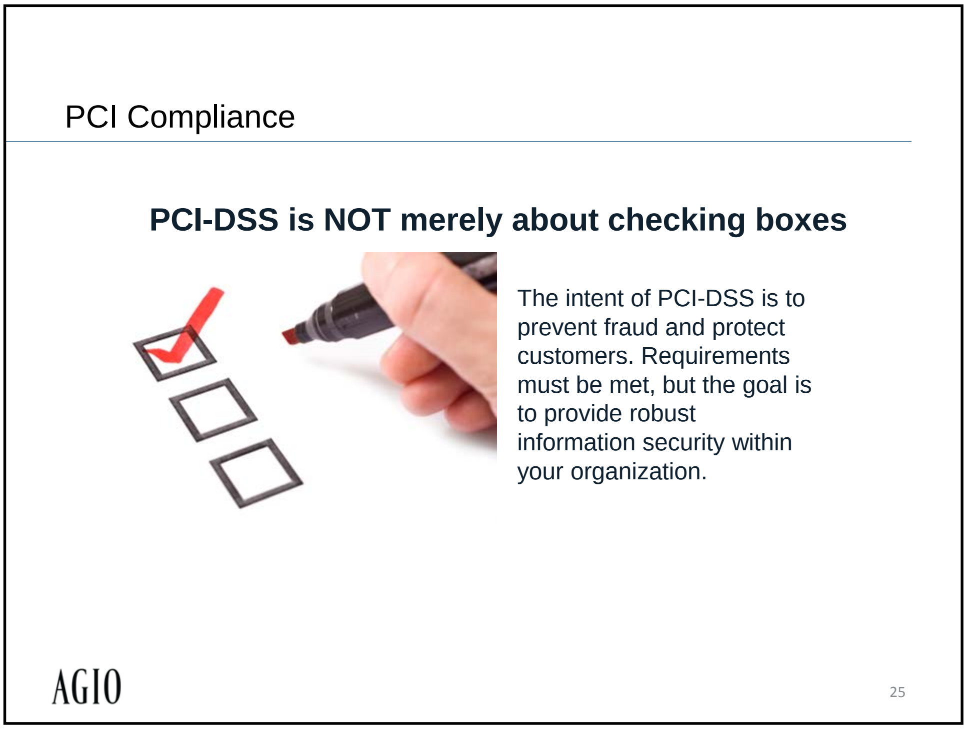


What Should I Do?

- Identify all payment channels (methods of processing payment)
  - Group the Merchant IDs MIDs
  - Location
  - Applications
  - Storage
- Identify all systems used in the process (scoping)
  - Asset inventory
- Conduct gap assessment
  - Apply the standard to the “in scope” systems

AGIO

24



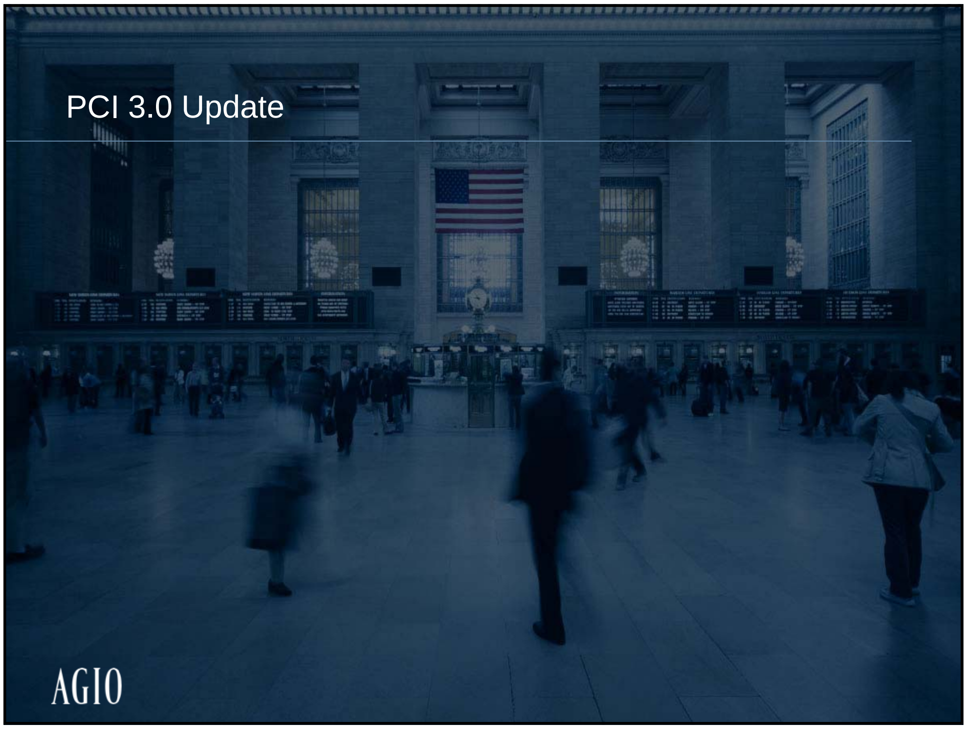
PCI Compliance

PCI-DSS is NOT merely about checking boxes

The intent of PCI-DSS is to prevent fraud and protect customers. Requirements must be met, but the goal is to provide robust information security within your organization.

AGIO

25



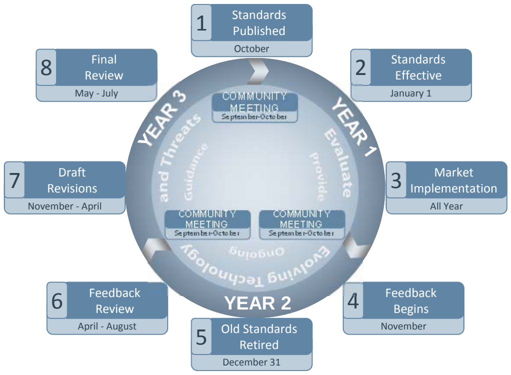
PCI 3.0 Update

AGIO

The PCI DSS Lifecycle

- The PCI DSS follows a three-year lifecycle
- PCI DSS 3.0 was released in October 2013
- Optional (but recommended) in 2014; Required in 2015

Lifecycle for Changes to PCI DSS and PA-DSS



1 Standards Published
October

2 Standards Effective
January 1

3 Market Implementation
All Year

4 Feedback Begins
November

5 Old Standards Retired
December 31

6 Feedback Review
April - August

7 Draft Revisions
November - April

8 Final Review
May - July

YEAR 1
Evaluate
Provide

YEAR 2
Evolving Technology
Ongoing

YEAR 3
and Threats
Guidance

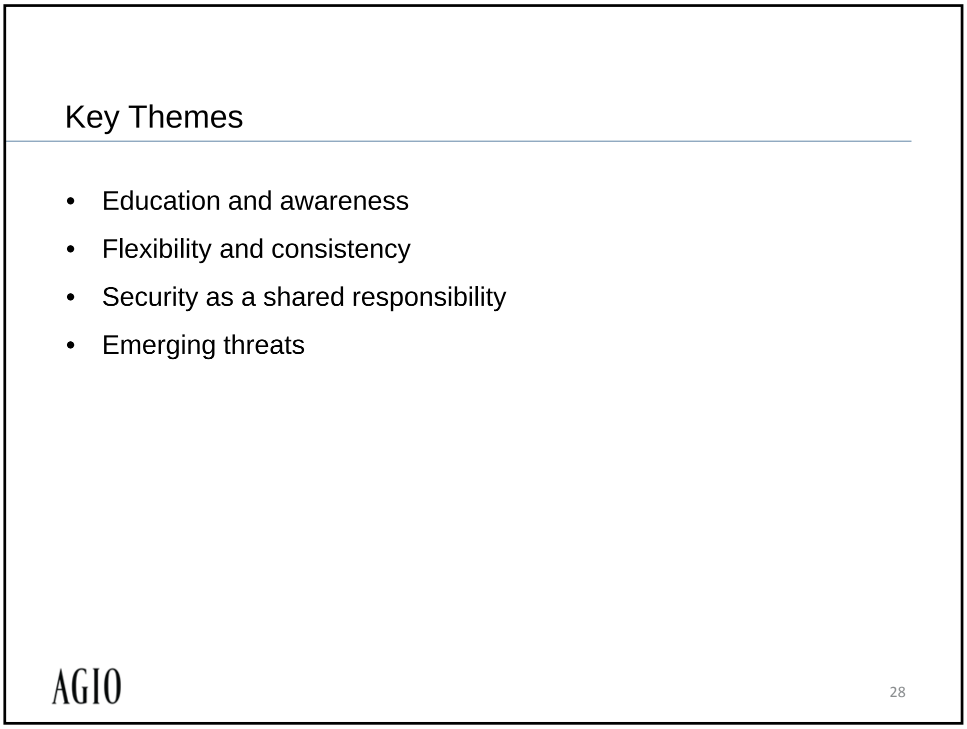
COMMUNITY MEETING
September-October

COMMUNITY MEETING
September-October

COMMUNITY MEETING
September-October

AGIO

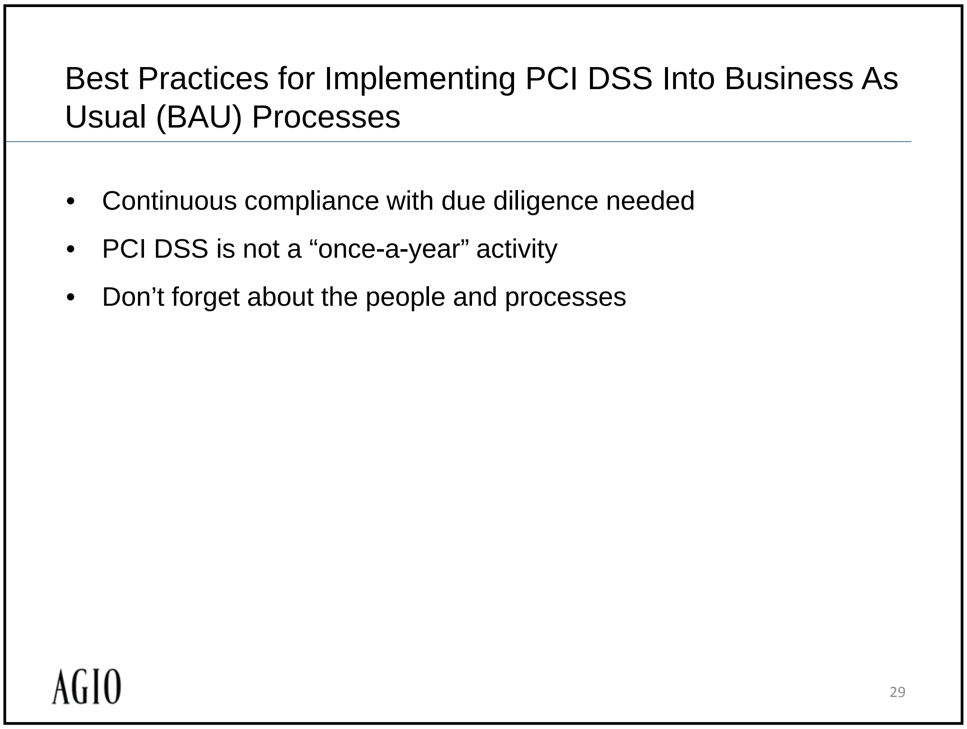
27



Key Themes

- Education and awareness
- Flexibility and consistency
- Security as a shared responsibility
- Emerging threats

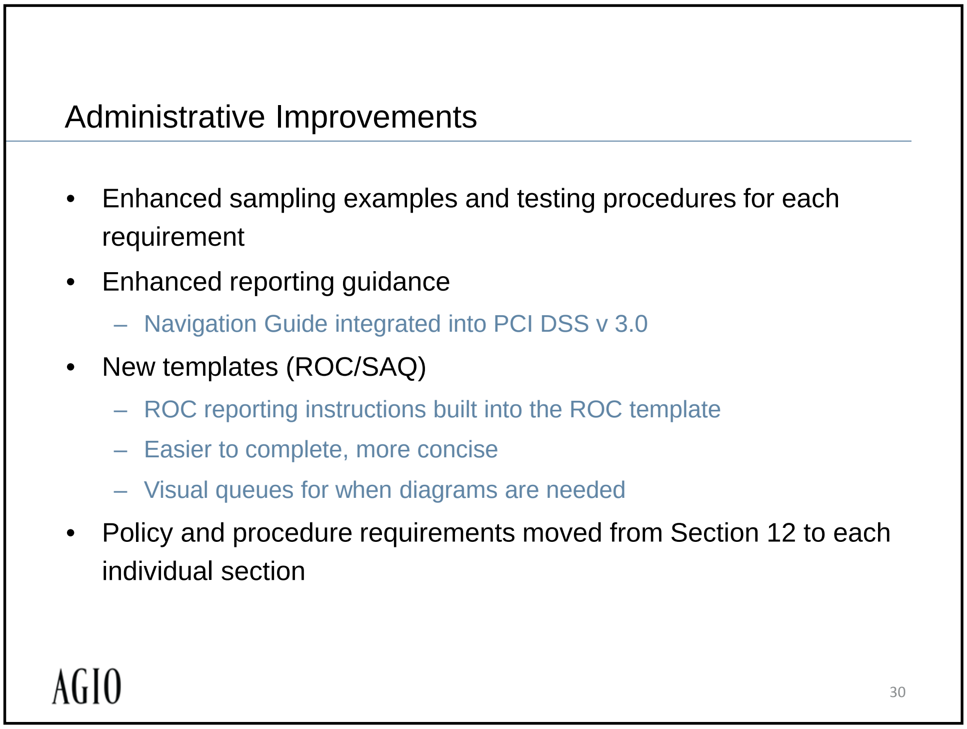
AGIO



Best Practices for Implementing PCI DSS Into Business As Usual (BAU) Processes

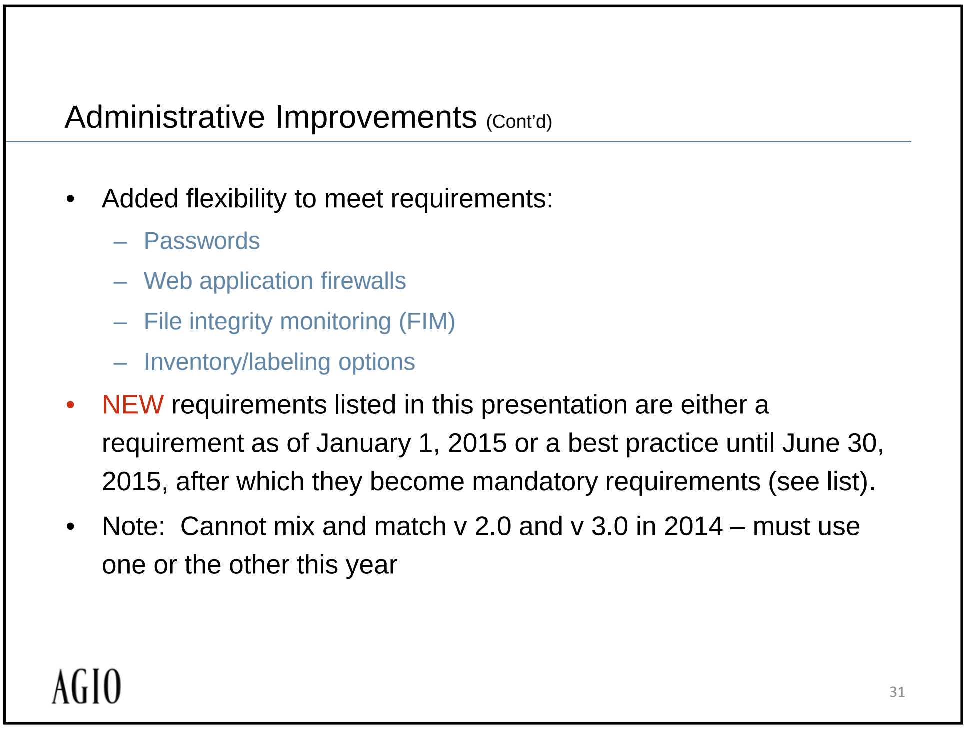
- Continuous compliance with due diligence needed
- PCI DSS is not a “once-a-year” activity
- Don’t forget about the people and processes

AGIO



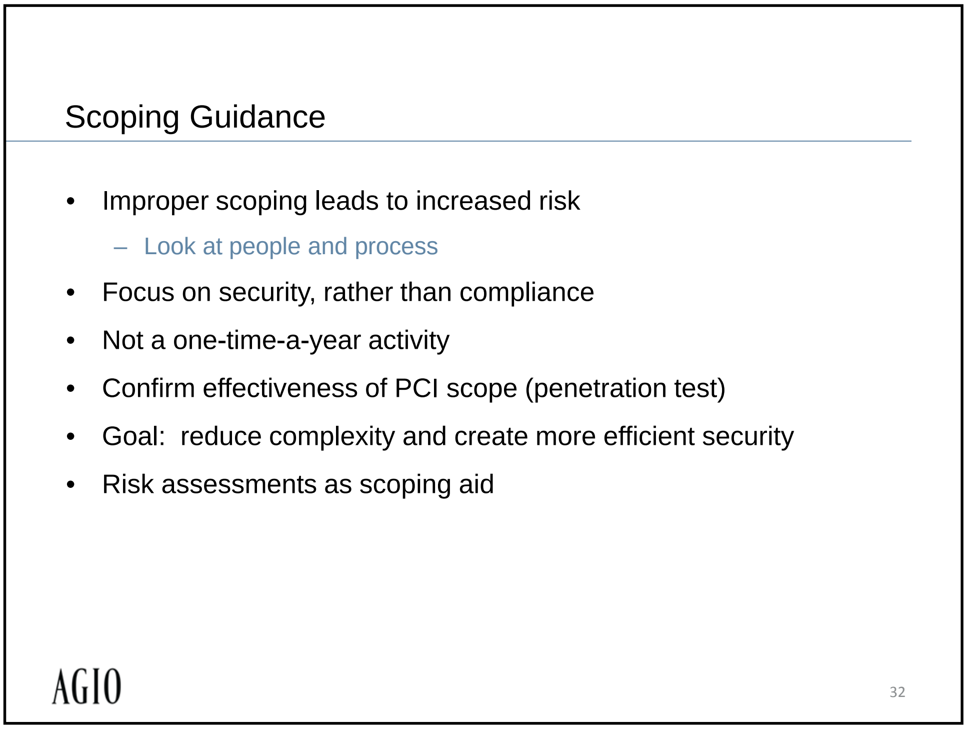
Administrative Improvements

- Enhanced sampling examples and testing procedures for each requirement
- Enhanced reporting guidance
  - Navigation Guide integrated into PCI DSS v 3.0
- New templates (ROC/SAQ)
  - ROC reporting instructions built into the ROC template
  - Easier to complete, more concise
  - Visual queues for when diagrams are needed
- Policy and procedure requirements moved from Section 12 to each individual section



Administrative Improvements (Cont'd)

- Added flexibility to meet requirements:
  - Passwords
  - Web application firewalls
  - File integrity monitoring (FIM)
  - Inventory/labeling options
- NEW requirements listed in this presentation are either a requirement as of January 1, 2015 or a best practice until June 30, 2015, after which they become mandatory requirements (see list).
- Note: Cannot mix and match v 2.0 and v 3.0 in 2014 – must use one or the other this year

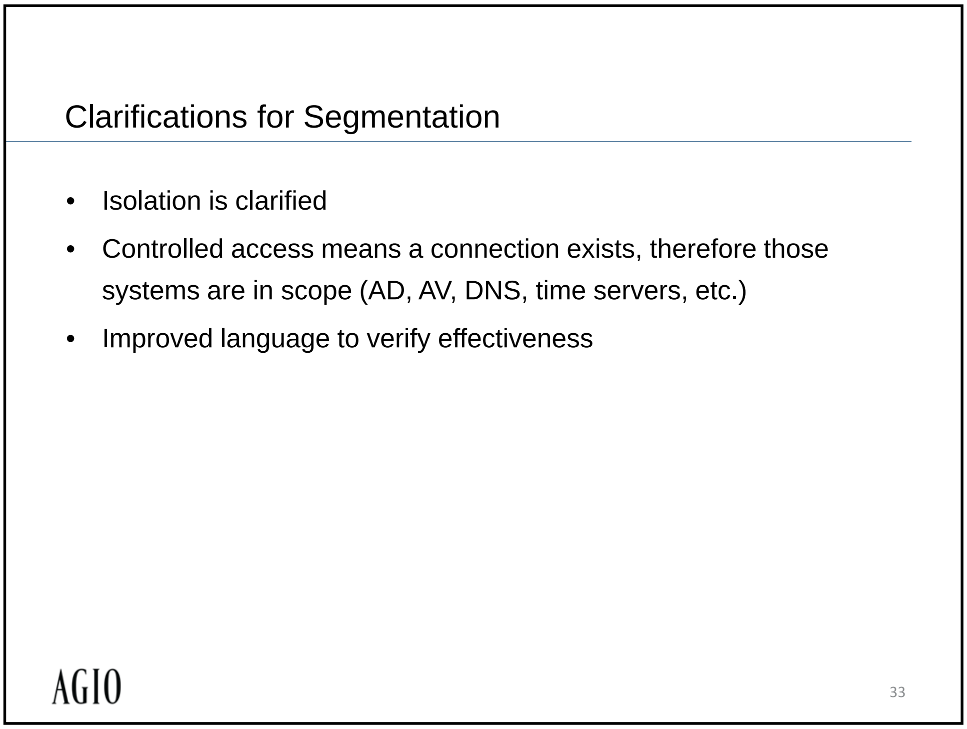


Scoping Guidance

- Improper scoping leads to increased risk
  - Look at people and process
- Focus on security, rather than compliance
- Not a one-time-a-year activity
- Confirm effectiveness of PCI scope (penetration test)
- Goal: reduce complexity and create more efficient security
- Risk assessments as scoping aid

AGIO

32

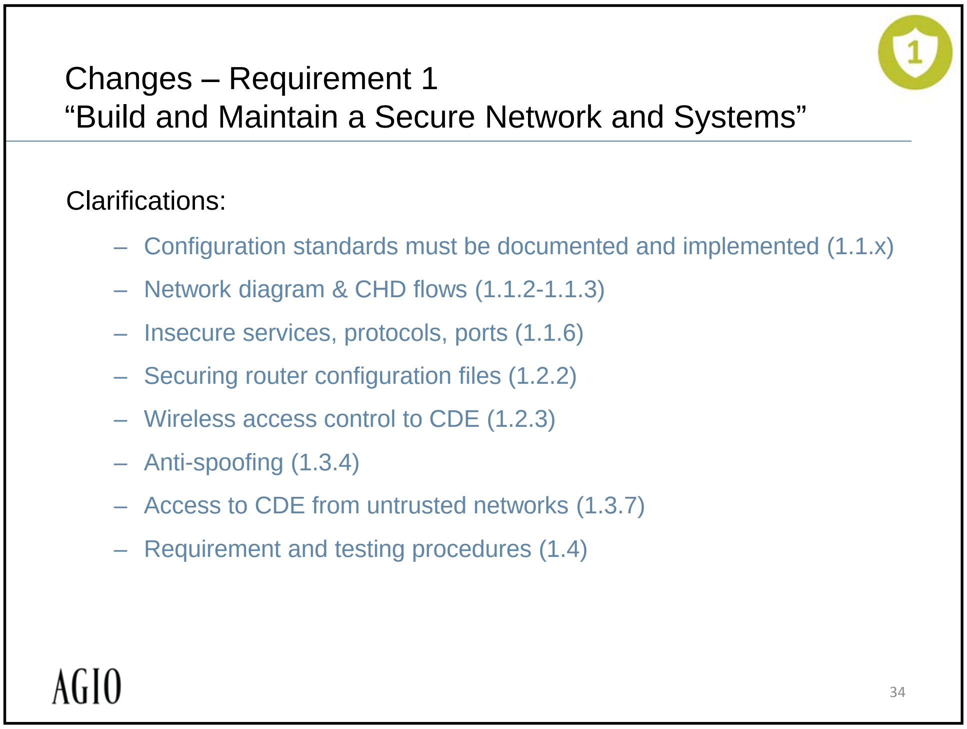


Clarifications for Segmentation

- Isolation is clarified
- Controlled access means a connection exists, therefore those systems are in scope (AD, AV, DNS, time servers, etc.)
- Improved language to verify effectiveness

AGIO

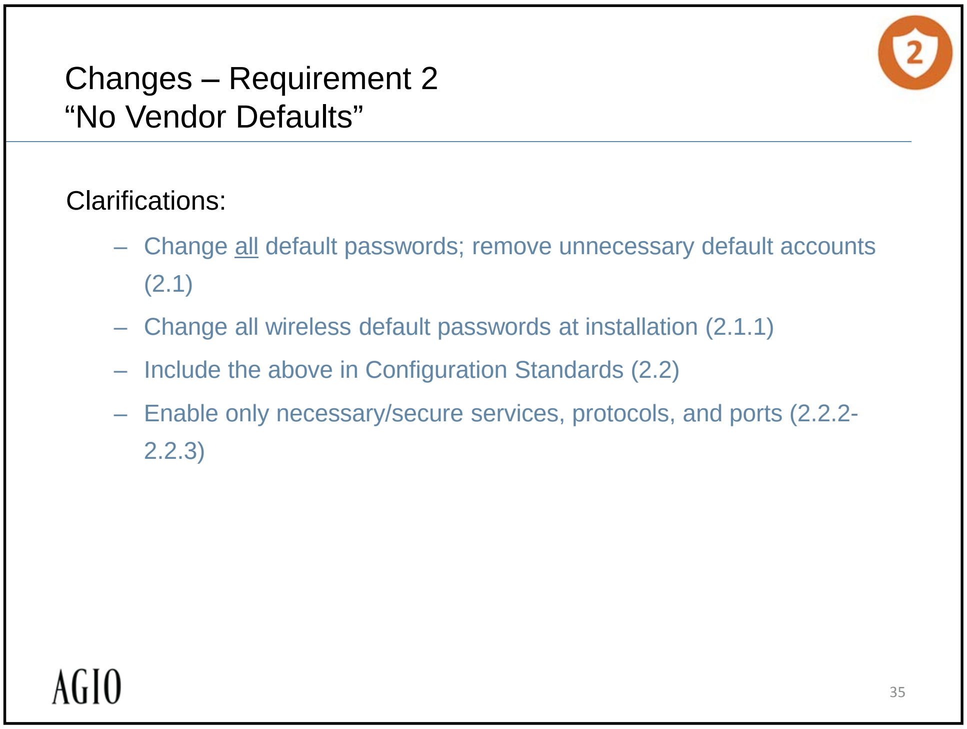
33



Changes – Requirement 1
“Build and Maintain a Secure Network and Systems”

Clarifications:

- Configuration standards must be documented and implemented (1.1.x)
- Network diagram & CHD flows (1.1.2-1.1.3)
- Insecure services, protocols, ports (1.1.6)
- Securing router configuration files (1.2.2)
- Wireless access control to CDE (1.2.3)
- Anti-spoofing (1.3.4)
- Access to CDE from untrusted networks (1.3.7)
- Requirement and testing procedures (1.4)



Changes – Requirement 2
“No Vendor Defaults”

Clarifications:

- Change all default passwords; remove unnecessary default accounts (2.1)
- Change all wireless default passwords at installation (2.1.1)
- Include the above in Configuration Standards (2.2)
- Enable only necessary/secure services, protocols, and ports (2.2.2-2.2.3)

Changes – Requirement 2
“No Vendor Defaults”

NEW Requirement:

REQUIRED BY JAN 1, 2015

- Maintain an inventory of all systems and components that are in scope for PCI DSS

Changes – Requirement 3
“Protect Stored Cardholder Data (CHD)”

Clarifications:

- Data Retention and Disposal (3.1.x)
- Sensitive Authentication Data (SAD) proper destruction after authorization (3.2)
- Primary Account Number (PAN) masking (3.3)
- Separation of OS and Disk-level encryption authentication mechanisms (3.4.1)
- Key Management procedures (3.5)
- Provided flexibility with more options for secure storage of cryptographic keys (3.5.2-3.5.3)
- Testing implementation of crypto key management (3.6.x)
- Crypto key “split-knowledge” and “key control” (3.6.6)

Changes – Requirement 4 "Encrypt Transmission of CHD Across Untrusted Networks"

4

Clarifications:

- Expanded examples of open public networks (4.1)

AGIO

Changes – Requirement 5 "Maintain a Vulnerability Management Program"

5

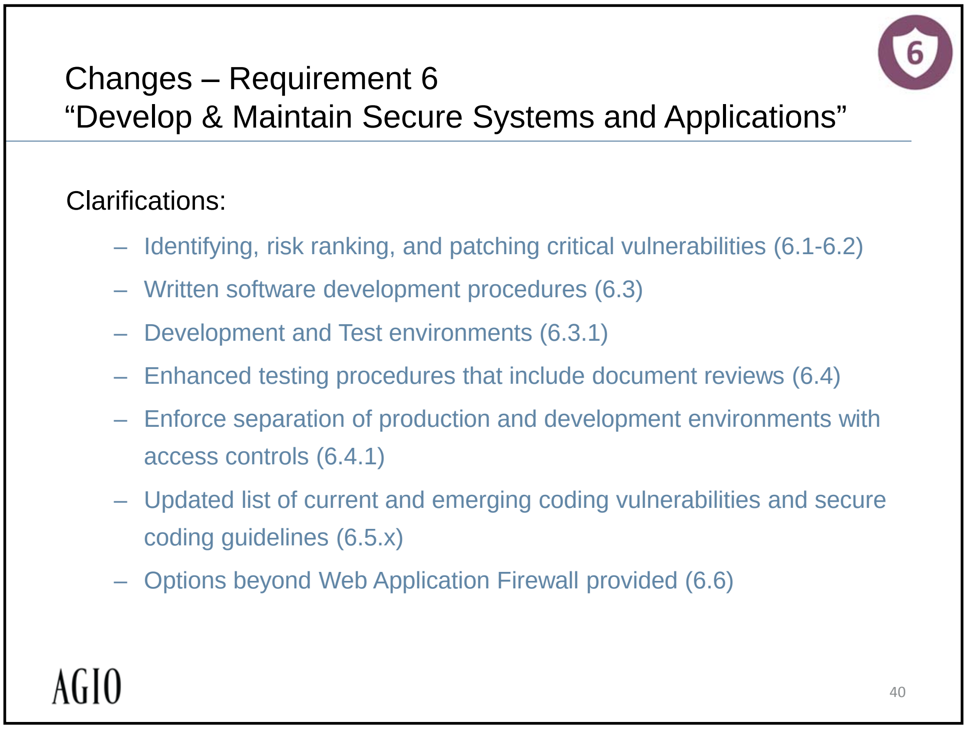
Clarifications:

- Ensure all AV mechanisms are maintained properly (5.2)

NEW Requirements:

- REQUIRED BY JAN 1, 2015 – Systems not commonly affected by malware must be evaluated (5.1.2)
- REQUIRED BY JAN 1, 2015 – Ensure AV is running and cannot be disabled/altered (5.3)

AGIO



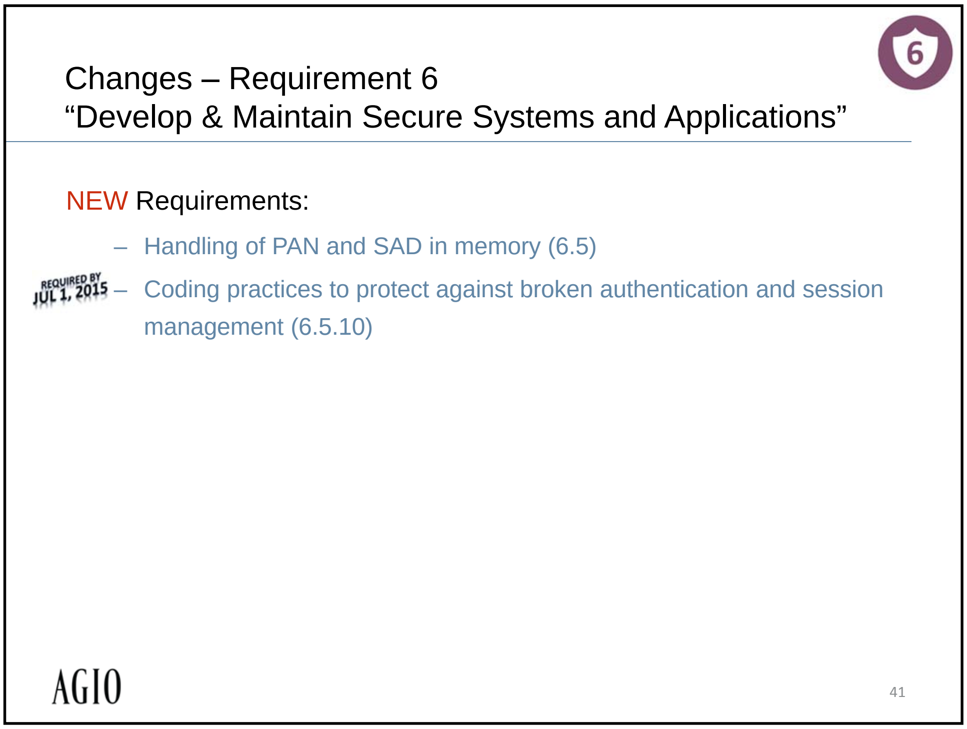
Changes – Requirement 6 “Develop & Maintain Secure Systems and Applications”

Clarifications:

- Identifying, risk ranking, and patching critical vulnerabilities (6.1-6.2)
- Written software development procedures (6.3)
- Development and Test environments (6.3.1)
- Enhanced testing procedures that include document reviews (6.4)
- Enforce separation of production and development environments with access controls (6.4.1)
- Updated list of current and emerging coding vulnerabilities and secure coding guidelines (6.5.x)
- Options beyond Web Application Firewall provided (6.6)

AGIO

40



Changes – Requirement 6 “Develop & Maintain Secure Systems and Applications”

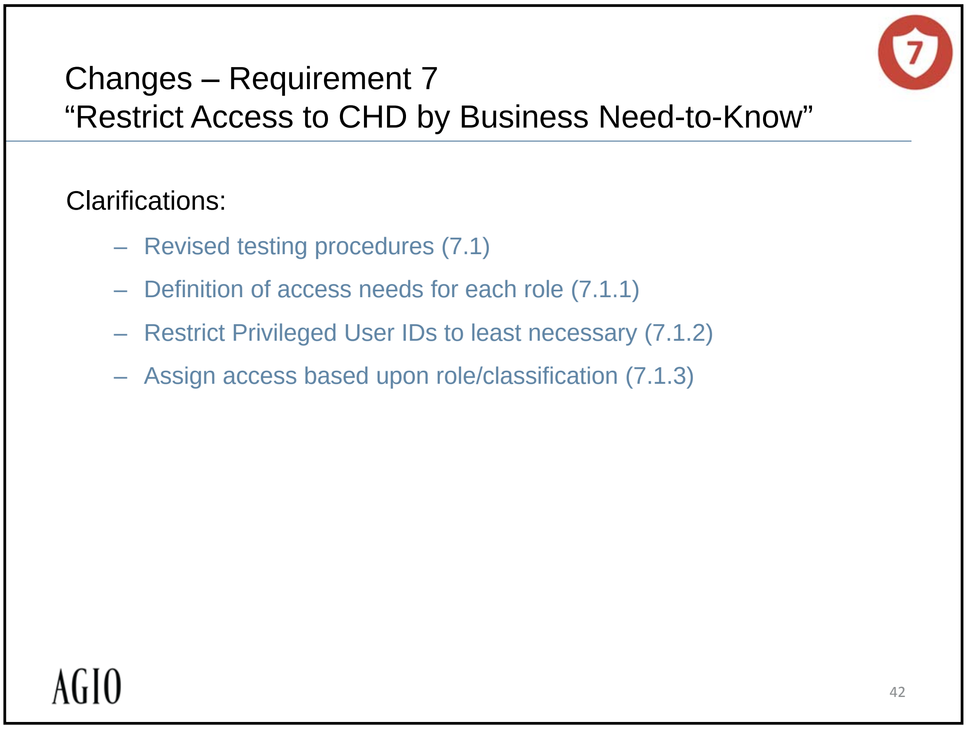
NEW Requirements:

- Handling of PAN and SAD in memory (6.5)
- Coding practices to protect against broken authentication and session management (6.5.10)

REQUIRED BY JUL 1, 2015

AGIO

41

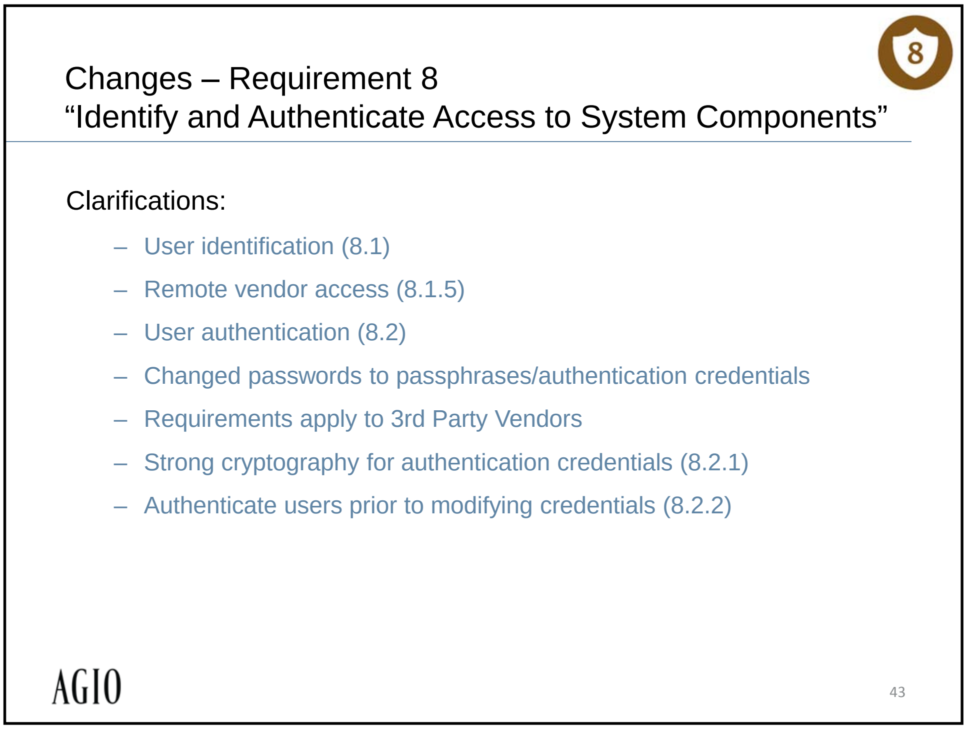


Changes – Requirement 7
“Restrict Access to CHD by Business Need-to-Know”

Clarifications:

- Revised testing procedures (7.1)
- Definition of access needs for each role (7.1.1)
- Restrict Privileged User IDs to least necessary (7.1.2)
- Assign access based upon role/classification (7.1.3)

AGIO

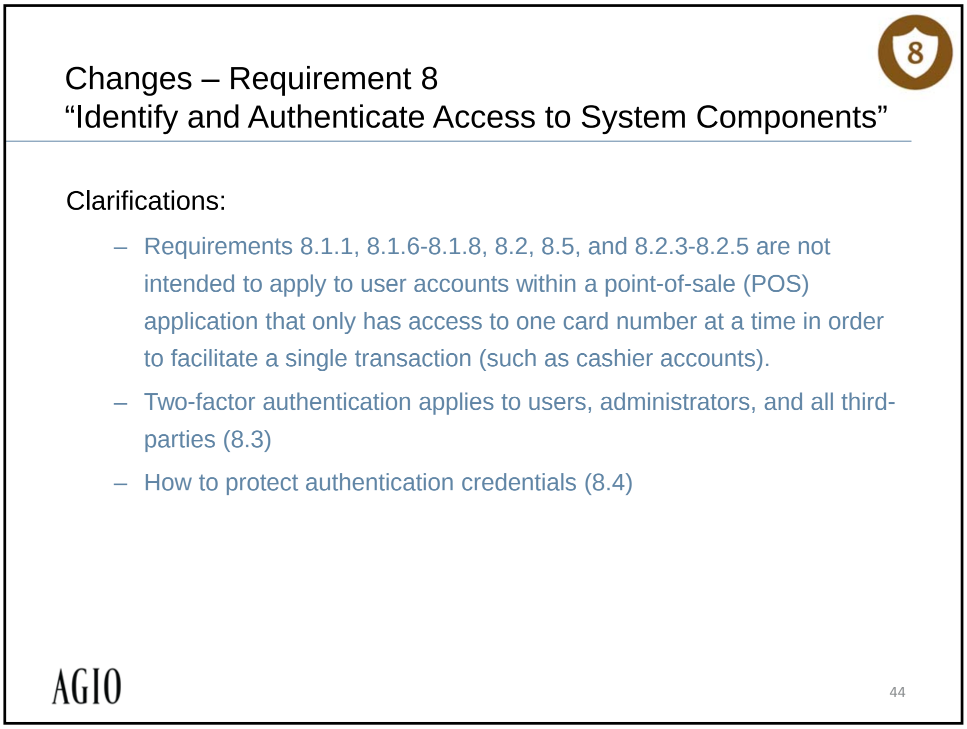


Changes – Requirement 8
“Identify and Authenticate Access to System Components”

Clarifications:

- User identification (8.1)
- Remote vendor access (8.1.5)
- User authentication (8.2)
- Changed passwords to passphrases/authentication credentials
- Requirements apply to 3rd Party Vendors
- Strong cryptography for authentication credentials (8.2.1)
- Authenticate users prior to modifying credentials (8.2.2)

AGIO



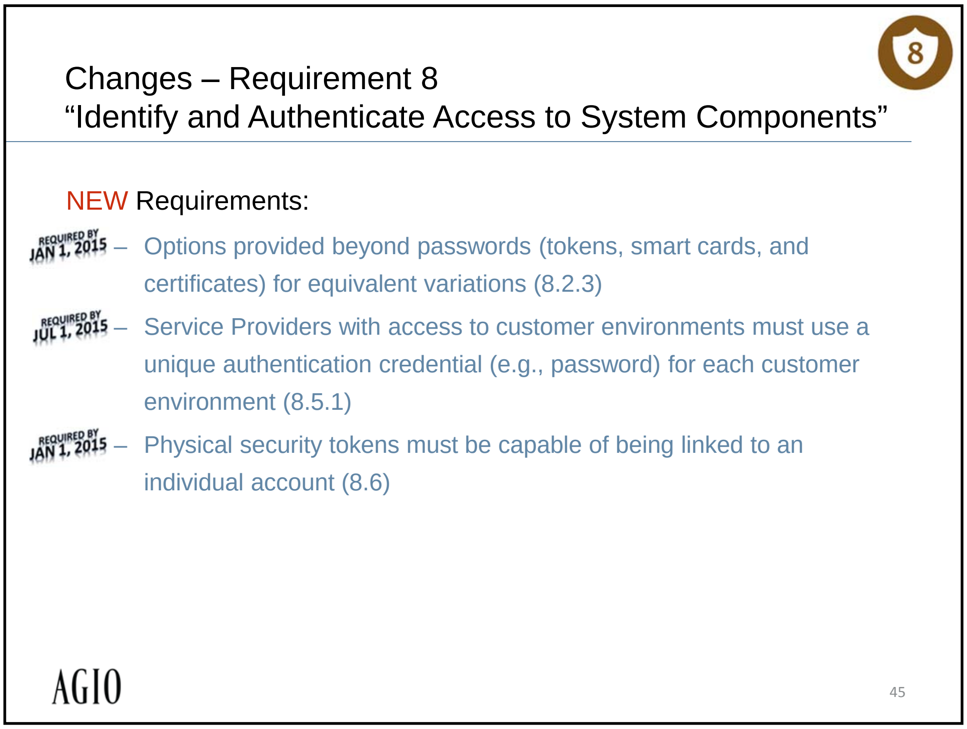
Changes – Requirement 8
“Identify and Authenticate Access to System Components”

Clarifications:

- Requirements 8.1.1, 8.1.6-8.1.8, 8.2, 8.5, and 8.2.3-8.2.5 are not intended to apply to user accounts within a point-of-sale (POS) application that only has access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).
- Two-factor authentication applies to users, administrators, and all third-parties (8.3)
- How to protect authentication credentials (8.4)

AGIO

44



Changes – Requirement 8
“Identify and Authenticate Access to System Components”

NEW Requirements:

- REQUIRED BY JAN 1, 2015 – Options provided beyond passwords (tokens, smart cards, and certificates) for equivalent variations (8.2.3)
- REQUIRED BY JUL 1, 2015 – Service Providers with access to customer environments must use a unique authentication credential (e.g., password) for each customer environment (8.5.1)
- REQUIRED BY JAN 1, 2015 – Physical security tokens must be capable of being linked to an individual account (8.6)

AGIO

45

Changes – Requirement 9
"Restrict Physical Access to Cardholder Data"

9

Clarifications:

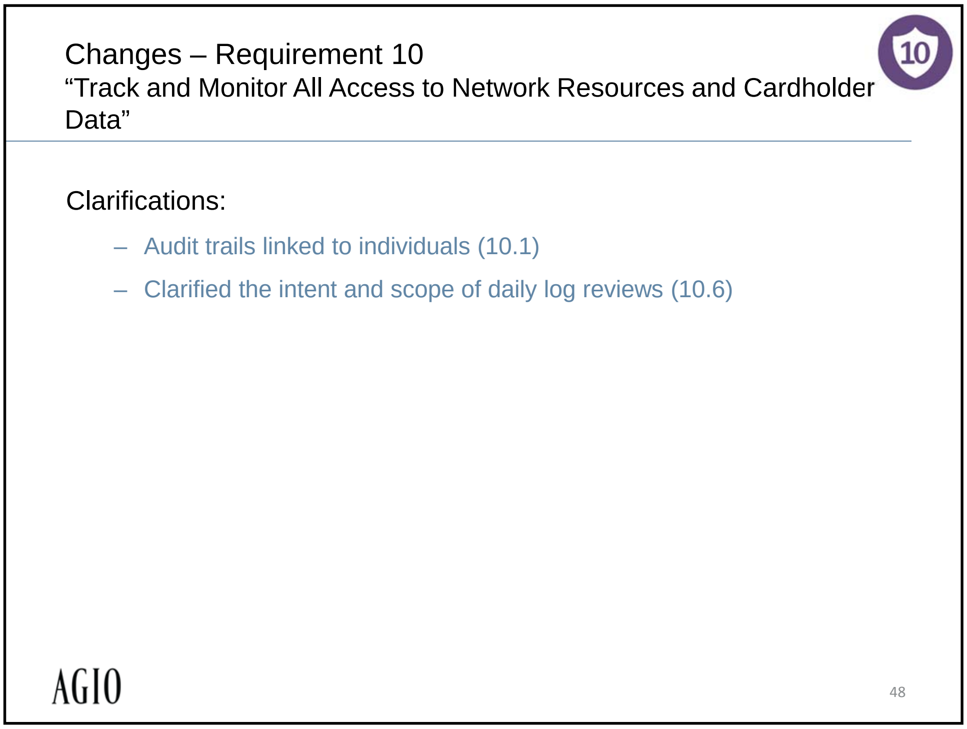
- Protection of network jacks (9.1.2)
- Differentiation between on-site personnel and visitors – options made available (9.2.x)
- Visitor audit trails (9.4.x)

Changes – Requirement 9
"Restrict Physical Access to Cardholder Data"

9

NEW Requirements:

- REQUIRED BY JAN 1, 2015 – Control physical access to sensitive areas for on-site personnel (9.3)
- REQUIRED BY JUL 1, 2015 – Protect POS terminals and devices from tampering or substitution (9.9)



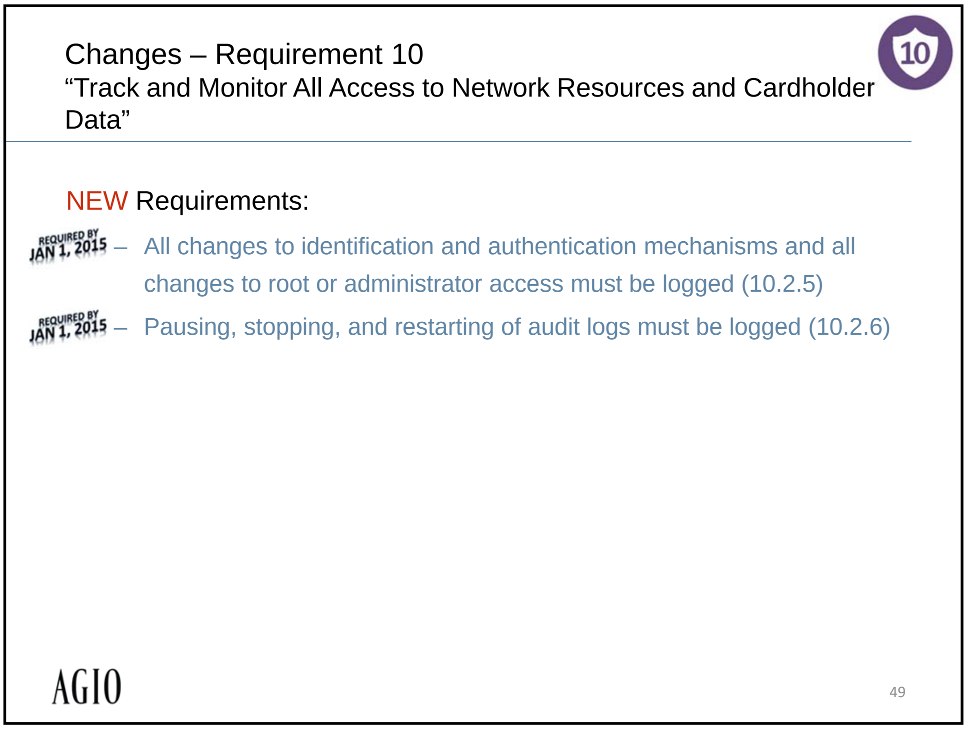
Changes – Requirement 10
“Track and Monitor All Access to Network Resources and Cardholder Data”

Clarifications:

- Audit trails linked to individuals (10.1)
- Clarified the intent and scope of daily log reviews (10.6)

AGIO

48



Changes – Requirement 10
“Track and Monitor All Access to Network Resources and Cardholder Data”

NEW Requirements:

- REQUIRED BY JAN 1, 2015 – All changes to identification and authentication mechanisms and all changes to root or administrator access must be logged (10.2.5)
- REQUIRED BY JAN 1, 2015 – Pausing, stopping, and restarting of audit logs must be logged (10.2.6)

AGIO

49

Changes – Requirement 11
"Regularly Test Security Systems and Processes"

Clarifications:

- Added guidance regarding multiple scan reports (11.2)
- Quarterly internal vulnerability scans must be repeated until a passing scan results (11.2.2)
- Internal and External scans must be performed after significant changes (11.2.3)
- Correct all vulnerabilities detected during a Penetration Test (11.3.3)
- Methods expanded for detecting changes to files (11.5)

AGIO

Changes – Requirement 11
"Regularly Test Security Systems and Processes"

NEW Requirements:

- REQUIRED BY JAN 1, 2015 – Have an inventory and business justification for wireless access points (11.1.x)
- REQUIRED BY JUL 1, 2015 – Implement a methodology for penetration testing, and perform penetration tests to verify that the segmentation methods are operational and effective (11.3)
- REQUIRED BY JAN 1, 2015 – Develop process to respond to change detection alerts (11.5.1)

AGIO

Changes – Requirement 12 “Maintain a Policy that Addresses Security for all Personnel”

12

Clarifications:

- Policy and procedure requirements moved from Section 12 to each individual section
- Added options regarding identification (labeling) of devices (12.3.4)
- Testing of remote access timeouts (12.3.8)
- Management of Service Providers (12.8)
- Further defined the components of Incident Response plan (12.10.x)

AGIO

52

Changes – Requirement 12 “Maintain a Policy that Addresses Security for all Personnel”

12

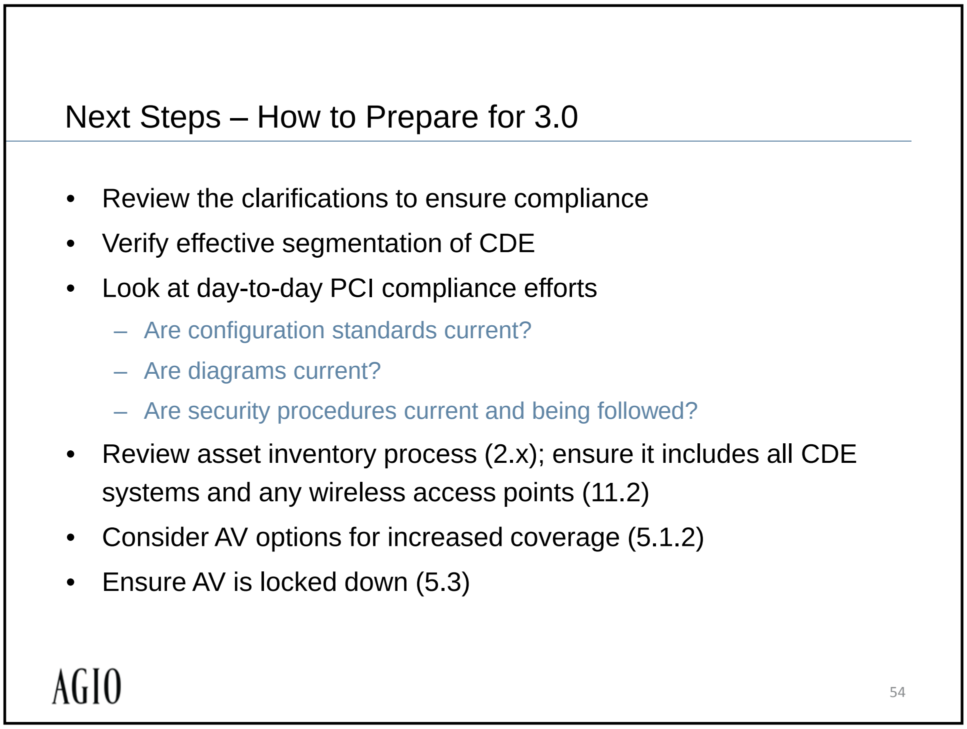
NEW Requirements:

- REQUIRED BY JAN 1, 2015 – Risk Assessment should be performed at least annually and after significant changes (12.2)
- REQUIRED BY JAN 1, 2015 – Maintain separation of duties for security responsibilities (12.4.1)
- REQUIRED BY JAN 1, 2015 – Clarified essential components of Service Provider agreements (12.8.2)
- REQUIRED BY JAN 1, 2015 – Maintain information about which PCI DSS requirements are managed by service providers and which are managed by the entity (12.8.5).
- Service providers to acknowl esponsibility for maintaining applicable PCI DSS requirements. (12.9)

REQUIRED BY JUL 1, 2015

AGIO

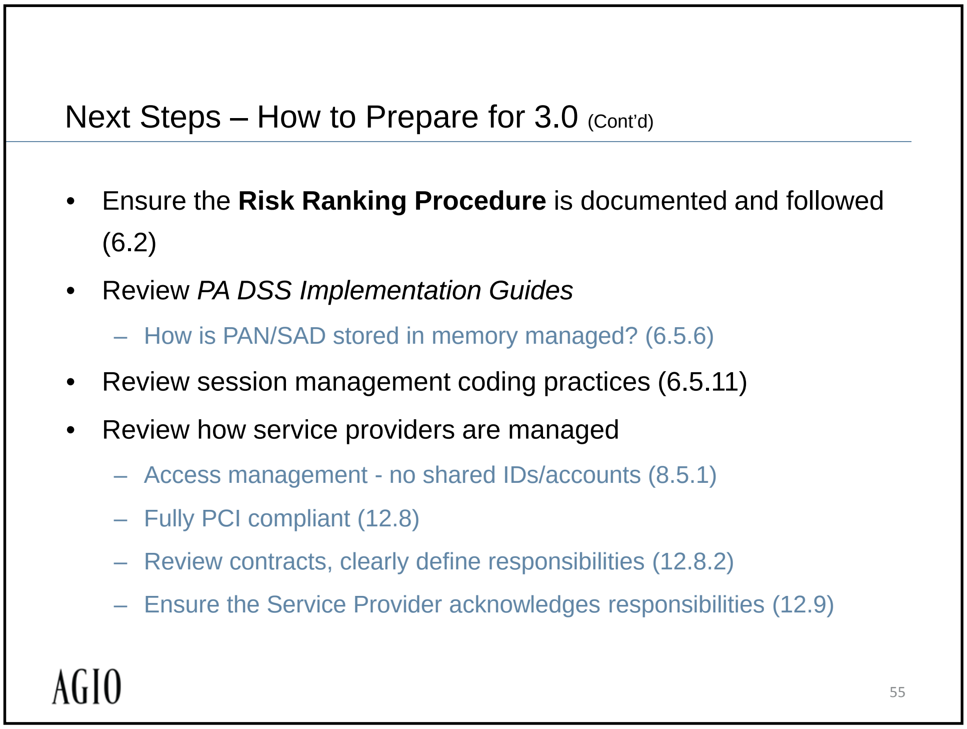
53



Next Steps – How to Prepare for 3.0

- Review the clarifications to ensure compliance
- Verify effective segmentation of CDE
- Look at day-to-day PCI compliance efforts
  - Are configuration standards current?
  - Are diagrams current?
  - Are security procedures current and being followed?
- Review asset inventory process (2.x); ensure it includes all CDE systems and any wireless access points (11.2)
- Consider AV options for increased coverage (5.1.2)
- Ensure AV is locked down (5.3)

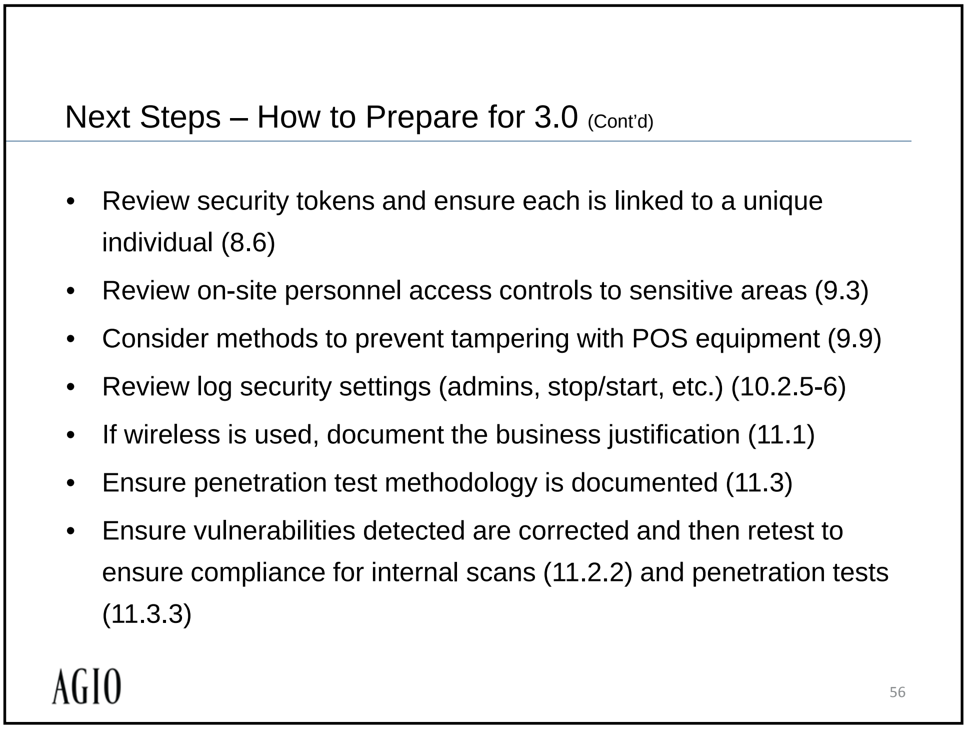
54



Next Steps – How to Prepare for 3.0 (Cont'd)

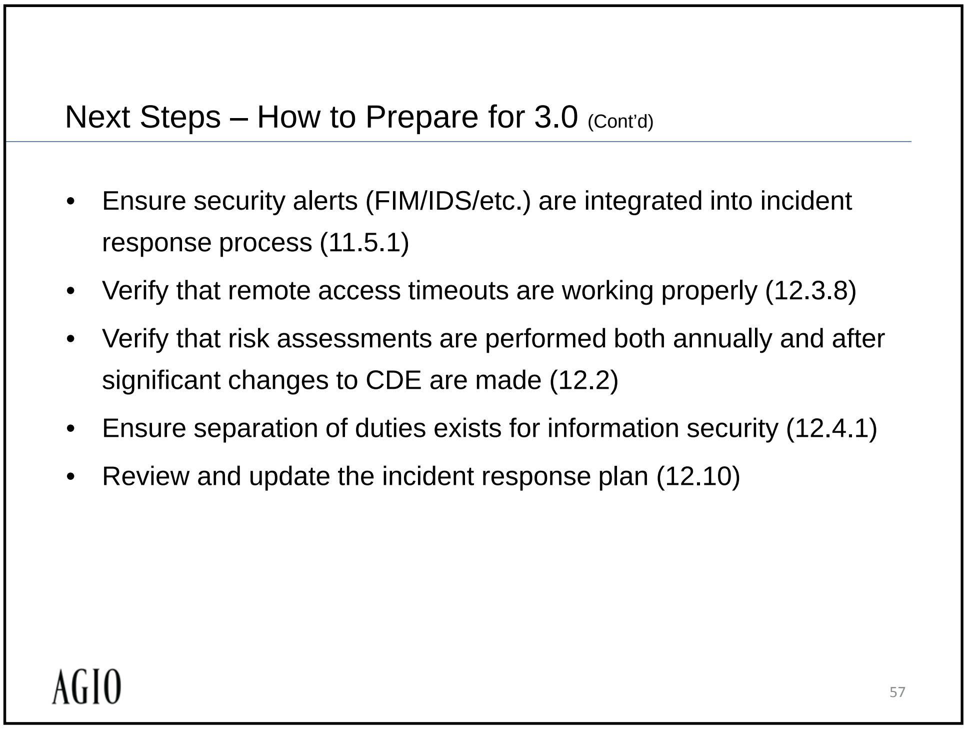
- Ensure the **Risk Ranking Procedure** is documented and followed (6.2)
- Review *PA DSS Implementation Guides*
  - How is PAN/SAD stored in memory managed? (6.5.6)
- Review session management coding practices (6.5.11)
- Review how service providers are managed
  - Access management - no shared IDs/accounts (8.5.1)
  - Fully PCI compliant (12.8)
  - Review contracts, clearly define responsibilities (12.8.2)
  - Ensure the Service Provider acknowledges responsibilities (12.9)

55



Next Steps – How to Prepare for 3.0 (Cont'd)

- Review security tokens and ensure each is linked to a unique individual (8.6)
- Review on-site personnel access controls to sensitive areas (9.3)
- Consider methods to prevent tampering with POS equipment (9.9)
- Review log security settings (admins, stop/start, etc.) (10.2.5-6)
- If wireless is used, document the business justification (11.1)
- Ensure penetration test methodology is documented (11.3)
- Ensure vulnerabilities detected are corrected and then retest to ensure compliance for internal scans (11.2.2) and penetration tests (11.3.3)



Next Steps – How to Prepare for 3.0 (Cont'd)

- Ensure security alerts (FIM/IDS/etc.) are integrated into incident response process (11.5.1)
- Verify that remote access timeouts are working properly (12.3.8)
- Verify that risk assessments are performed both annually and after significant changes to CDE are made (12.2)
- Ensure separation of duties exists for information security (12.4.1)
- Review and update the incident response plan (12.10)

Questions?

PCI Security Awareness Training

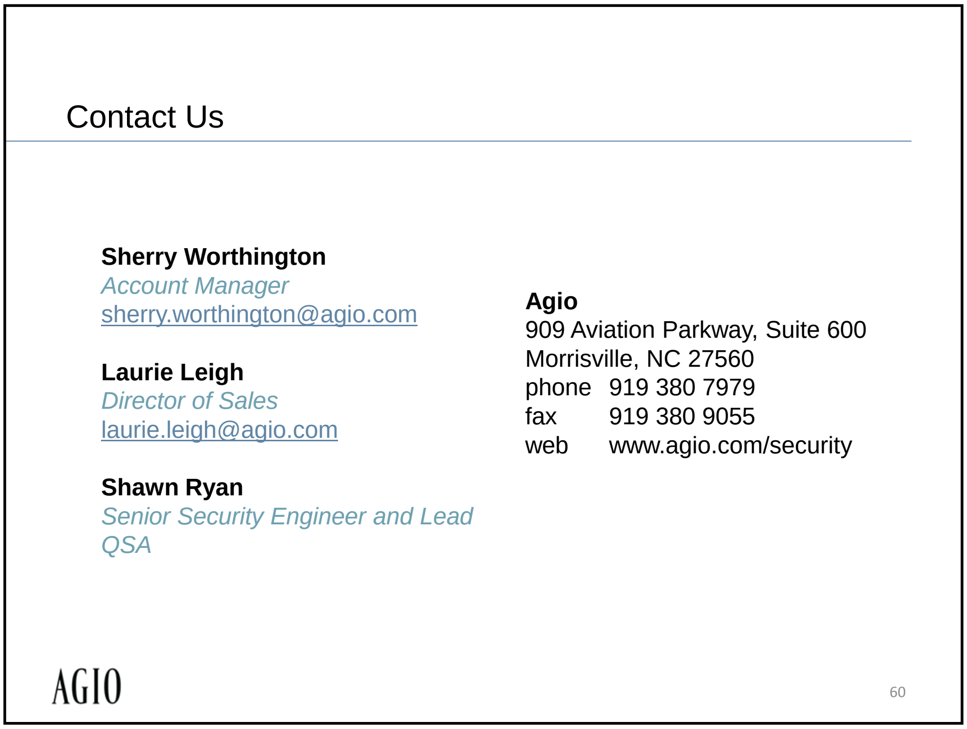
Thank you!

Agio has performed network and application security assessments for over 14 years. Agio is recognized by the Payment Card Industry Security Standards Council (PCI SSC) as both a Qualified Security Assessor (QSA) and an Approved Scanning Vendor (ASV).

We are happy to help you with any and all compliance efforts.

919 380 7979

Agio | **agio.com/security**



Contact Us

Sherry Worthington
Account Manager
sherry.worthington@agio.com

Laurie Leigh
Director of Sales
laurie.leigh@agio.com

Shawn Ryan
Senior Security Engineer and Lead QSA

Agio
909 Aviation Parkway, Suite 600
Morrisville, NC 27560

phone	919 380 7979
fax	919 380 9055
web	www.agio.com/security

eCommerce
From Paper to Electronic
April 30, 2014

Attendees by Last Name (321)

Bennie Aiken—Department of Insurance
David Alford—Department of Transportation
Robert Alford—Office of the State Controller
Shelly Alman—Gaston College
Rebecca Anderson—Rowan-Cabarrus Community College
Lewis Andrews—Department of State Treasurer
Debora Antley—Office of Information Technology Services
Michael Arnold—Department of Secretary of the State
Deborah Atkinson—Department of Health and Human Services
Khalid Awan—Department of Public Safety
Phillip Ayscue—Department of Transportation
Debra Bailey—East Carolina University
Jennifer Baird—Department of Agriculture
Rita Baker—Department of State Treasurer
William Ball—Administrative Office of the Courts
John Barfield—Office of the State Controller
Deborah Barnes—Department of Health and Human Services
Angela Barrett—Office of the State Controller
Julie Batchelor—Office of the State Controller
Sheila Bell—City of Monroe
Joseph Belnak—NC Education Lottery
Thomas Berryman—Department of Health and Human Services
Jeannie Betts—Department of Environment and Natural Resources
Eric Blaize—Department of Secretary of the State
David Blakemore—UNC at Chapel Hill
Brian Bothern—NC Community College System
Dee Bowling—East Carolina University
Eric Boyette—Department of Transportation
Bryan Brannon—Administrative Office of the Courts
Nancy Brendell—Western Carolina University
Brian Bridgers—NC Community College System
Jack Brinson—Department of Labor
Robert Brinson—Department of Public Safety
Madelene Brooks—Cape Fear Community College
Ricky Brown—Pitt Community College
Helen Buck—NC A and T State University
Michelle Burks—Department of Health and Human Services
George Burnette—UNC School of the Arts
Mary "Ellen" Burns—Department of Commerce
Norman Burtness—Department of Secretary of the State
Timothy Byrd—UNC Hospitals
Edith Cannady—Office of the State Controller
Charles Cansler—NC State University
Wynona Cash—Office of the State Controller
Debbie Cashwell—Richmond Community College
Dewey "EDDY" Cavenaugh—UNC School of the Arts
Taylor Chappell—NC State University
Tommy Clark—Wildlife Resources Commission
Emily Coble—UNC at Chapel Hill
Elizabeth Colcord—Department of Revenue
Ivanna Cole—NC Central University
Stephanie Coleman—East Carolina University
Cindy Collie—Alamance Community College
Kevin Crutchfield—NC State University
Dewanda Dalrymple—NC Central University
Clayton Darnell—Office of the State Controller
Amanda Davis—UNC Hospitals
Angie Davis—UNC at Chapel Hill
Diane Davis—NC A and T State University
Rod Davis—Department of Health and Human Services
Steven Davis—Department of Public Safety
Joyce Davis-Freeman—Dept. of Environmental and Natural Resources
Robin Deaver—Fayetteville Technical Community College
Yolanda Deaver—NC Central University
Joseph DeBragga—Department of Environment and Natural Resources
James DeFrancisco—Department of Public Safety
Carmelitta DeGraffinreed—County of Wake
John DelGreco—Department of Public Safety
Jay Deming—Department of Transportation
George Dennis—NC Administrative Office of the Courts
Mike Dickerson—NC State University
Debbie Dryer—Office of the State Controller
Angela DuBose—NC A and T State University
Iona Duckworth—State Education Assistance Authority
Kenneth Durham—Department of State Treasurer
Michael Durkin—Department of Transportation
Deborah Edelman—Department of Environment and Natural Resources
Cecilia Edgar—Wildlife Resources Commission
Bivian Ejimakor—NC A and T State University
Wendy Emerson—Forsyth Technical Community College
Leah Englebright—NC School of Science and Mathematics
Laresia Everett—Department of Insurance
Roger Farmer—Office of the State Controller
Melissa Fenton—Rex Healthcare
Joanne Ferguson—UNC at Wilmington
Nadine Flint—UNC at Wilmington
Cliff Flood—UNC General Administration
Susan Flowers—Department of Environment and Natural Resources
Carol Fornes—East Carolina University
Craig Forsythe—Office of Information Technology Services
Mark Foster—Department of Transportation
Pam Fowler—Office of the State Controller
Patricia Fritz—East Carolina University
Linda Fuller—Department of Transportation
Samiel Fuller—Department of Public Instruction
Jennifer Gamiel—Department of Environment and Natural Resources
Linda Garr—Rex Healthcare
Tami George—Robeson Community College
Peggy Gill—Department of Transportation
Anne Godwin—Office of the State Controller
Bonnie Godwin—Department of Agriculture
Laura Gore—UNC at Wilmington
Martha Greene—Forsyth Technical Community College
Angela Griffin—Office of State Budget and Management
Wendy Griffin—Department of Transportation
A.J. Hafele—UNC Chapel Hill
Clay Hallock—East Carolina University
Elizabeth Hammond—Office of the Commissioner of Banks
Keith Hammonds—Department of Public Safety
Brenda Hampshire—UNC at Greensboro
Brian Harper—Department of Labor
Carol Harris—NC Central University
Haley Haynes—Department of Secretary of the State
Clayton Heath—Department of Transportation
Thomas Henry—Halifax Community College
Clay Hicks—County of Guilford
Freda Hilburn—Department of Commerce
Regina Hill—Office of State Budget and Management
Alonzo Hines—NC A and T State University
Matt Hinnant—UNC at Wilmington
Shannon Hobby—Department of Commerce
Pat Holcomb—Department of Secretary of the State
Susan Holton—NCSU
Jason Holtz—Department of Labor
Donald Hoover—Department of Commerce
James Horne—NC General Assembly Program Evaluation Division
Heather Horton—Department of Environment and Natural Resources
William Hosterman—UNC Hospitals
Troy Howell—UNC at Chapel Hill
Larry Huffman—Department of Health and Human Services
Scott Hummel—NC A and T State University
Heather Hummer—UNC General Administration
Heather Iannucci—UNC at Wilmington
Suzanne Imboden—East Carolina University
Ken Ingle—Rowan-Cabarrus Community College
Carmin Ipock—East Carolina University
Rokos Isaak—Office of the State Controller
Denise Jackson—Department of Public Instruction
David Jamison—Appalachian State University
Lars Jarkko—UNC General Administration
Bud Jennings—Administrative Office of the Courts
Patricia Jeter—NC Utilities Commission
Elizabeth John—Department of Justice
Sherrilyn Johnson—East Carolina University
Angela Johnston—Office of the State Controller
Christine Jonas—Craven Community College
Audrey Jones—Town Of Apex
Joanne Jones—UNC at Greensboro
Sue Kearney—Department of Agriculture
Robin Kee—UNC at Wilmington
Keyana Kimbrough—UNC at Chapel Hill
John Kincaid—Office of the State Controller
Stephanie King—Department of Transportation
Bliss Kite—Department of Commerce
Andrew Kleitsch—Durham Technical Community College
Laura Klem—Office of the State Controller
Mark Kozel—UNC at Chapel Hill
Stan Koziol—UNC at Chapel Hill
Roxanne Krotoszynski—Department of Health and Human Services
Beth Lane—Pitt Community College
Karin Langbehn-Pecaut—UNC at Chapel Hill
Darlene Langston—Department of Public Safety
Betty Larose—Office of Information Technology Services
Robin Larson—UNC Hospitals
Michelle Lassiter—NC Education Lottery
Kizzy Lea—Rowan-Cabarrus Community College
Angie Leary—Department of Environment and Natural Resources
Tracey Lemming—UNC at Chapel Hill
Gayle Lemons—Office of Administrative Hearings
Stratton Lindley—Department of Transportation
Cathy Lively—Office of Information Technology Services
Curtis Long—Department of Transportation
Frank Lord—Winston-Salem State University

Summer Lowe—Department of Environment and Natural Resources
Becky Luce-Clark—Department of Justice
Tami Luckwaldt—Department of Insurance
David Lucus—NC Central University
Kathleen Lukens—UNC at Greensboro
Karen Main—Appalachian State University
Diana Malinsky—UNC at Chapel Hill
Jeff Marecic—Administrative Office of the Courts
Duane Maxie—NC Community College System
Kenny Maye—NC A and T State University
Charlotte Maynard—Department of Public Safety
Robin Mayo—East Carolina University
Marcus McAllister—Office of the State Controller
Cameron McCall—Wildlife Resources Commission
Amy McCauley—Wake Technical Community College
Cynthia McCrory—Gaston College
Susan McCullen—County of Wake
Renetta McEachern—Department of Secretary of the State
Jackie McKoy—Department of Revenue
Ben McLawhorn—Office of the State Controller
Adrienne McLean—Department of Labor
Kelly Merrell—UNC Hospitals
Jolene Meyer—State Education Assistance Authority
Cindy Meyers—Department of Environment and Natural Resources
Laketha Miller—Department of Health and Human Services
Marvin Miller—Martin Community College
Mary Mims—NC A and T State University
Janet Mintern—NC Community College System
Kelly Mogle—UNC Hospitals
Lee Montrose—Richmond Community College
Todd Morgan—Department of Transportation
Tim Morris—East Carolina University
Daryl Morrison—Department of Revenue
Dannie Moss—East Carolina University
Claire Mufalo—NC Central University
Clayton Murphy—Office of the State Controller
Lettie Navarrete—Robeson Community College
Debra Neal—Department of Administration
Shannon Newlin—Alamance Community College
Jim Newman—Office of Secretary of State
David Nicolaysen—Department of Transportation
Terri Noblin—Office of the State Controller
Liza Nordstrom—NC Community College System
Hans Norland—Department of Public Safety
Nancy Norris—Western Piedmont Community College
Gwen Norwood—UNC at Chapel Hill
Tony Norwood—Department of Administration
Melanie Nuckols—Forsyth Technical Community College
Terri Overton—Department of Agriculture
Ray Oxendine—UNC at Pembroke
Jennifer Pacheco—Office of the State Controller
Padmashree Paluri—Office of Information Technology Services
Bridget Paschal—Department of Commerce
Tracy Patty—NC State University
Chris Pearce—Forsyth Technical Community College
Patty Peebles—East Carolina University
Gary Penrod—UNC School of the Arts
Amy Penson—Isothermal Community College
Barbara Perkins—Office of the State Controller
Johnny Peterson—Craven Community College
Michelle Phillips—NC State University
Tina Pickett—Department of Health and Human Services
Rick Pieringer—Office of the State Controller
Cathy Piner—NC Aquarium at Pine Knoll Shores
Randall Powell—UNC at Charlotte
Belinda Preacher—Department of Secretary of the State
Rick Presnell—Appalachian State University
Dennis Press—UNC at Chapel Hill
David Price—East Carolina University
Phillip Price—Central Carolina Community College
Dawn Quist—East Carolina University
Chandrika Rao—UNC at Chapel Hill
Pasupula Ravindranath—UNC Hospitals
David Reavis—UNC - FIT
Pyreddy Reddy—Department of Health and Human Services
Kathryn Reeves—Cape Fear Community College
Stephen Reeves—NC Community College System
Cindy Revels—UNC at Pembroke
Camellia Rice—Cape Fear Community College
Javier Rivera—Department of Health and Human Services
Beth Roberts—Department of Justice
Jeremy Roberts—Office of the State Controller
Priscilla Roberts—Department of Secretary of the State
Sherry Robertson—Tri-County Community College
Al Roethlisberger—Department of Transportation
Jessica Rogers—Blue Ridge Community College
Scott Rogers—Caldwell Community College
Elizabeth Rollinson—USS North Carolina Battleship Commission
Janet Rust—Department of Labor
Camilla Sandlin—NC Education Lottery
Lei Satterfield—Department of Revenue
Joan Saucier—Department of Public Safety
William Schmidt—Department of Commerce
Troy Scoggins—Department of Health and Human Services
Teresa Shingleton—Office of the State Controller
Jon B Sholar—East Carolina University
Holly Silvey—Fayetteville Technical Community College
Vanessa Singletary—Robeson Community College
Betty Smith—Fayetteville Technical Community College
Charles Smith—Fayetteville Technical Community College
Debra Smith—Halifax Community College
Juliana Smith—Office of Information Technology Services
Randy Smith—Wildlife Resources Commission
Rod Smith—UNC - Chapel Hill
Ron Smith—UNC at Greensboro
Patricia "Pat" Stanley—UNC at Chapel Hill
Faye Steele—East Carolina University
Kathleen Stefanick—NC State University
Karen Stevenson—UNC at Greensboro
Sharon Stevenson—UNC General Administration
Danny Stewart—Department of Health and Human Services
David Stone—Department of Transportation
Mike Suggs—NC Education Lottery
Michael Sullivan—Rex Healthcare
Michele Sykes—Office of State Budget and Management
Sharon Tanner—Department of Revenue
Marla Tart—Wake Technical Community College
Greg Taylor—NC Aquarium at Pine Knoll Shores
Lisa Taylor—UNC at Chapel Hill
Karen Thiessen—County of Wake
Nancy Thomas—Office of the State Controller
Randy Thomas—Office of the State Controller
Debbie Todd—Fayetteville Technical Community College
Shawn Toderick—Forsyth Technical Community College
Diep Tong—Central Piedmont Community College
Shirley Trollinger—Office of the State Controller
Christopher Tyler—Department of Public Safety
Stormy Van Hees—Department of Justice
Kim VanMetre—Office of Information Technology Services
Page Varnell—Craven Community College
Melody Vaughn—UNC Hospitals
Suma Vempa—Office of the State Controller
Prabhavathi Vijayaraghavan—Office of the State Controller
Megan Wallace—UNC at Chapel Hill
Adam Ward—Alamance Community College
Gary Ward—NC Central University
Rex Whaley—Department of Environment and Natural Resources
Margie Whitfield—Department of Health and Human Services
Eddie Whittington—NC Aquarium Society
LaToya Wiley—UNC School of the Arts
James Willamor—Stanly Community College
Susan Williams—UNC at Chapel Hill
Joe Wilson Jr—Department of Transportation
Frank Winn—Department of Transportation
Jennifer Wooten—Office of the State Controller
Tracey Yarborough—Pitt Community College
Willard Young—Department of Transportation
Joanna Zazzali—Department of Environment and Natural Resources

eCommerce
From Paper to Electronic
April 30, 2014

Attendees by Agency (321)

William Ball—Administrative Office of the Courts
Bryan Brannon—Administrative Office of the Courts
Bud Jennings—Administrative Office of the Courts
Jeff Marecic—Administrative Office of the Courts
Cindy Collie—Alamance Community College
Shannon Newlin—Alamance Community College
Adam Ward—Alamance Community College
David Jamison—Appalachian State University
Karen Main—Appalachian State University
Rick Presnell—Appalachian State University
Jessica Rogers—Blue Ridge Community College
Scott Rogers—Caldwell Community College
Madelene Brooks—Cape Fear Community College
Kathryn Reeves—Cape Fear Community College
Camellia Rice—Cape Fear Community College
Phillip Price—Central Carolina Community College
Diep Tong—Central Piedmont Community College
Sheila Bell—City of Monroe
Clay Hicks—County of Guilford
Carmelitta DeGraffinreed—County of Wake
Susan McCullen—County of Wake
Karen Thiessen—County of Wake
Christine Jonas—Craven Community College
Johnny Peterson—Craven Community College
Page Varnell—Craven Community College
Debra Neal—Department of Administration
Tony Norwood—Department of Administration
Jennifer Baird—Department of Agriculture
Bonnie Godwin—Department of Agriculture
Sue Kearney—Department of Agriculture
Terri Overton—Department of Agriculture
Mary "Ellen" Burns—Department of Commerce
Freda Hilburn—Department of Commerce
Shannon Hobby—Department of Commerce
Donald Hoover—Department of Commerce
Bliss Kite—Department of Commerce
Bridget Paschal—Department of Commerce
William Schmidt—Department of Commerce
Jeannie Betts—Department of Environment and Natural Resources
Joseph DeBragga—Department of Environment and Natural Resources
Deborah Edelman—Department of Environment and Natural Resources
Susan Flowers—Department of Environment and Natural Resources
Jennifer Gamiel—Department of Environment and Natural Resources
Heather Horton—Department of Environment and Natural Resources
Angie Leary—Department of Environment and Natural Resources
Summer Lowe—Department of Environment and Natural Resources
Cindy Meyers—Department of Environment and Natural Resources
Rex Whaley—Department of Environment and Natural Resources
Joanna Zazzali—Department of Environment and Natural Resources
Deborah Atkinson—Department of Health and Human Services
Deborah Barnes—Department of Health and Human Services
Thomas Berryman—Department of Health and Human Services
Michelle Burks—Department of Health and Human Services
Rod Davis—Department of Health and Human Services
Larry Huffman—Department of Health and Human Services
Roxanne Krotoszynski—Department of Health and Human Services
Laketha Miller—Department of Health and Human Services
Tina Pickett—Department of Health and Human Services
Pyreddy Reddy—Department of Health and Human Services
Javier Rivera—Department of Health and Human Services
Troy Scoggins—Department of Health and Human Services
Danny Stewart—Department of Health and Human Services
Margie Whitfield—Department of Health and Human Services
Bennie Aiken—Department of Insurance
Laresia Everett—Department of Insurance
Tami Luckwaldt—Department of Insurance
Elizabeth John—Department of Justice
Becky Luce-Clark—Department of Justice
Beth Roberts—Department of Justice
Stormy Van Hees—Department of Justice
Jack Brinson—Department of Labor
Brian Harper—Department of Labor
Jason Holtz—Department of Labor
Adrienne McLean—Department of Labor
Janet Rust—Department of Labor
Samiel Fuller—Department of Public Instruction
Denise Jackson—Department of Public Instruction
Khalid Awan—Department of Public Safety
Robert Brinson—Department of Public Safety
Steven Davis—Department of Public Safety
James DeFrancisco—Department of Public Safety
John DelGreco—Department of Public Safety
Keith Hammonds—Department of Public Safety
Darlene Langston—Department of Public Safety
Charlotte Maynard—Department of Public Safety
Hans Norland—Department of Public Safety
Joan Saucier—Department of Public Safety
Christopher Tyler—Department of Public Safety
Elizabeth Colcord—Department of Revenue
Jackie McKoy—Department of Revenue
Daryl Morrison—Department of Revenue
Lei Satterfield—Department of Revenue
Sharon Tanner—Department of Revenue
Michael Arnold—Department of Secretary of the State
Eric Blaize—Department of Secretary of the State
Norman Burtness—Department of Secretary of the State
Haley Haynes—Department of Secretary of the State
Pat Holcomb—Department of Secretary of the State
Renetta McEachern—Department of Secretary of the State
Belinda Preacher—Department of Secretary of the State
Priscilla Roberts—Department of Secretary of the State
Lewis Andrews—Department of State Treasurer
Rita Baker—Department of State Treasurer
Kenneth Durham—Department of State Treasurer
David Alford—Department of Transportation
Phillip Ayscue—Department of Transportation
Eric Boyette—Department of Transportation
Jay Deming—Department of Transportation
Michael Durkin—Department of Transportation
Mark Foster—Department of Transportation
Linda Fuller—Department of Transportation
Peggy Gill—Department of Transportation
Wendy Griffin—Department of Transportation
Clayton Heath—Department of Transportation
Stephanie King—Department of Transportation
Stratton Lindley—Department of Transportation
Curtis Long—Department of Transportation
Todd Morgan—Department of Transportation
David Nicolaysen—Department of Transportation
Al Roethlisberger—Department of Transportation
David Stone—Department of Transportation
Joe Wilson Jr—Department of Transportation
Frank Winn—Department of Transportation
Willard Young—Department of Transportation
Joyce Davis-Freeman—Dept. of Environmental and Natural Resources
Andrew Kleitsch—Durham Technical Community College
Debra Bailey—East Carolina University
Dee Bowling—East Carolina University
Stephanie Coleman—East Carolina University
Carol Fornes—East Carolina University
Patricia Fritz—East Carolina University
Clay Hallock—East Carolina University
Suzanne Imboden—East Carolina University
Carmin Ipock—East Carolina University
Sherrilyn Johnson—East Carolina University
Robin Mayo—East Carolina University
Tim Morris—East Carolina University
Dannie Moss—East Carolina University
Patty Peebles—East Carolina University
David Price—East Carolina University
Dawn Quist—East Carolina University
Jon B Sholar—East Carolina University
Faye Steele—East Carolina University
Robin Deaver—Fayetteville Technical Community College
Holly Silvey—Fayetteville Technical Community College
Betty Smith—Fayetteville Technical Community College
Charles Smith—Fayetteville Technical Community College
Debbie Todd—Fayetteville Technical Community College
Wendy Emerson—Forsyth Technical Community College
Martha Greene—Forsyth Technical Community College
Melanie Nuckols—Forsyth Technical Community College
Chris Pearce—Forsyth Technical Community College
Shawn Toderick—Forsyth Technical Community College
Shelly Alman—Gaston College
Cynthia McCrory—Gaston College
Thomas Henry—Halifax Community College
Debra Smith—Halifax Community College
Amy Penson—Isothermal Community College
Marvin Miller—Martin Community College
Helen Buck—NC A and T State University
Diane Davis—NC A and T State University
Angela DuBose—NC A and T State University
Bivian Ejimakor—NC A and T State University
Alonzo Hines—NC A and T State University
Scott Hummel—NC A and T State University
Kenny Maye—NC A and T State University
Mary Mims—NC A and T State University
George Dennis—NC Administrative Office of the Courts
Cathy Piner—NC Aquarium at Pine Knoll Shores

Greg Taylor—NC Aquarium at Pine Knoll Shores
Eddie Whittington—NC Aquarium Society
Ivanna Cole—NC Central University
Dewanda Dalrymple—NC Central University
Yolanda Deaver—NC Central University
Carol Harris—NC Central University
David Lucus—NC Central University
Claire Mufalo—NC Central University
Gary Ward—NC Central University
Brian Bothern—NC Community College System
Brian Bridgers—NC Community College System
Duane Maxie—NC Community College System
Janet Mintern—NC Community College System
Liza Nordstrom—NC Community College System
Stephen Reeves—NC Community College System
Joseph Belnak—NC Education Lottery
Michelle Lassiter—NC Education Lottery
Camilla Sandlin—NC Education Lottery
Mike Suggs—NC Education Lottery
James Horne—NC General Assembly Program Evaluation Division
Leah Englebright—NC School of Science and Mathematics
Charles Cansler—NC State University
Taylor Chappell—NC State University
Kevin Crutchfield—NC State University
Mike Dickerson—NC State University
Tracy Patty—NC State University
Michelle Phillips—NC State University
Kathleen Stefanick—NC State University
Patricia Jeter—NC Utilities Commission
Susan Holton—NCSU
Gayle Lemons—Office of Administrative Hearings
Debora Antley—Office of Information Technology Services
Craig Forsythe—Office of Information Technology Services
Betty Larose—Office of Information Technology Services
Cathy Lively—Office of Information Technology Services
Padmashree Paluri—Office of Information Technology Services
Juliana Smith—Office of Information Technology Services
Kim VanMetre—Office of Information Technology Services
Jim Newman—Office of Secretary of State
Angela Griffin—Office of State Budget and Management
Regina Hill—Office of State Budget and Management
Michele Sykes—Office of State Budget and Management
Elizabeth Hammond—Office of the Commissioner of Banks
Robert Alford—Office of the State Controller
John Barfield—Office of the State Controller
Angela Barrett—Office of the State Controller
Julie Batchelor—Office of the State Controller
Edith Cannady—Office of the State Controller
Wynona Cash—Office of the State Controller
Clayton Darnell—Office of the State Controller
Debbie Dryer—Office of the State Controller
Roger Farmer—Office of the State Controller
Pam Fowler—Office of the State Controller
Anne Godwin—Office of the State Controller
Rokos Isaak—Office of the State Controller
Angela Johnston—Office of the State Controller
John Kincaid—Office of the State Controller
Laura Klem—Office of the State Controller
Marcus McAllister—Office of the State Controller
Ben McLawhorn—Office of the State Controller
Clayton Murphy—Office of the State Controller
Terri Noblin—Office of the State Controller
Jennifer Pacheco—Office of the State Controller
Barbara Perkins—Office of the State Controller
Rick Pieringer—Office of the State Controller
Jeremy Roberts—Office of the State Controller
Teresa Shingleton—Office of the State Controller
Nancy Thomas—Office of the State Controller
Randy Thomas—Office of the State Controller
Shirley Trollinger—Office of the State Controller
Suma Vempa—Office of the State Controller
Prabhavathi Vijayaraghavan—Office of the State Controller
Jennifer Wooten—Office of the State Controller
Ricky Brown—Pitt Community College
Beth Lane—Pitt Community College
Tracey Yarborough—Pitt Community College
Melissa Fenton—Rex Healthcare
Linda Garr—Rex Healthcare
Michael Sullivan—Rex Healthcare
Debbie Cashwell—Richmond Community College
Lee Montrose—Richmond Community College
Tami George—Robeson Community College
Lettie Navarrete—Robeson Community College
Vanessa Singletary—Robeson Community College
Rebecca Anderson—Rowan-Cabarrus Community College
Ken Ingle—Rowan-Cabarrus Community College
Kizzy Lea—Rowan-Cabarrus Community College
James Willamor—Stanly Community College
Iona Duckworth—State Education Assistance Authority
Jolene Meyer—State Education Assistance Authority
Audrey Jones—Town Of Apex
Sherry Robertson—Tri-County Community College
Rod Smith—UNC - Chapel Hill
David Reavis—UNC - FIT
David Blakemore—UNC at Chapel Hill
Emily Coble—UNC at Chapel Hill
Angie Davis—UNC at Chapel Hill
Troy Howell—UNC at Chapel Hill
Keyana Kimbrough—UNC at Chapel Hill
Mark Kozel—UNC at Chapel Hill
Stan Koziol—UNC at Chapel Hill
Karin Langbehn-Pecaut—UNC at Chapel Hill
Tracey Lemming—UNC at Chapel Hill
Diana Malinsky—UNC at Chapel Hill
Gwen Norwood—UNC at Chapel Hill
Dennis Press—UNC at Chapel Hill
Chandrika Rao—UNC at Chapel Hill
Patricia "Pat" Stanley—UNC at Chapel Hill
Lisa Taylor—UNC at Chapel Hill
Megan Wallace—UNC at Chapel Hill
Susan Williams—UNC at Chapel Hill
Randall Powell—UNC at Charlotte
Brenda Hampshire—UNC at Greensboro
Joanne Jones—UNC at Greensboro
Kathleen Lukens—UNC at Greensboro
Ron Smith—UNC at Greensboro
Karen Stevenson—UNC at Greensboro
Ray Oxendine—UNC at Pembroke
Cindy Revels—UNC at Pembroke
Joanne Ferguson—UNC at Wilmington
Nadine Flint—UNC at Wilmington
Laura Gore—UNC at Wilmington
Matt Hinnant—UNC at Wilmington
Heather Iannucci—UNC at Wilmington
Robin Kee—UNC at Wilmington
A.J. Hafele—UNC Chapel Hill
Cliff Flood—UNC General Administration
Heather Hummer—UNC General Administration
Lars Jarkko—UNC General Administration
Sharon Stevenson—UNC General Administration
Timothy Byrd—UNC Hospitals
Amanda Davis—UNC Hospitals
William Hosterman—UNC Hospitals
Robin Larson—UNC Hospitals
Kelly Merrell—UNC Hospitals
Kelly Mogle—UNC Hospitals
Pasupula Ravindranath—UNC Hospitals
Melody Vaughn—UNC Hospitals
George Burnette—UNC School of the Arts
Dewey "EDDY" Cavenaugh—UNC School of the Arts
Gary Penrod—UNC School of the Arts
LaToya Wiley—UNC School of the Arts
Elizabeth Rollinson—USS North Carolina Battleship Commission
Amy McCauley—Wake Technical Community College
Marla Tart—Wake Technical Community College
Nancy Brendell—Western Carolina University
Nancy Norris—Western Piedmont Community College
Tommy Clark—Wildlife Resources Commission
Cecilia Edgar—Wildlife Resources Commission
Cameron McCall—Wildlife Resources Commission
Randy Smith—Wildlife Resources Commission
Frank Lord—Winston-Salem State University