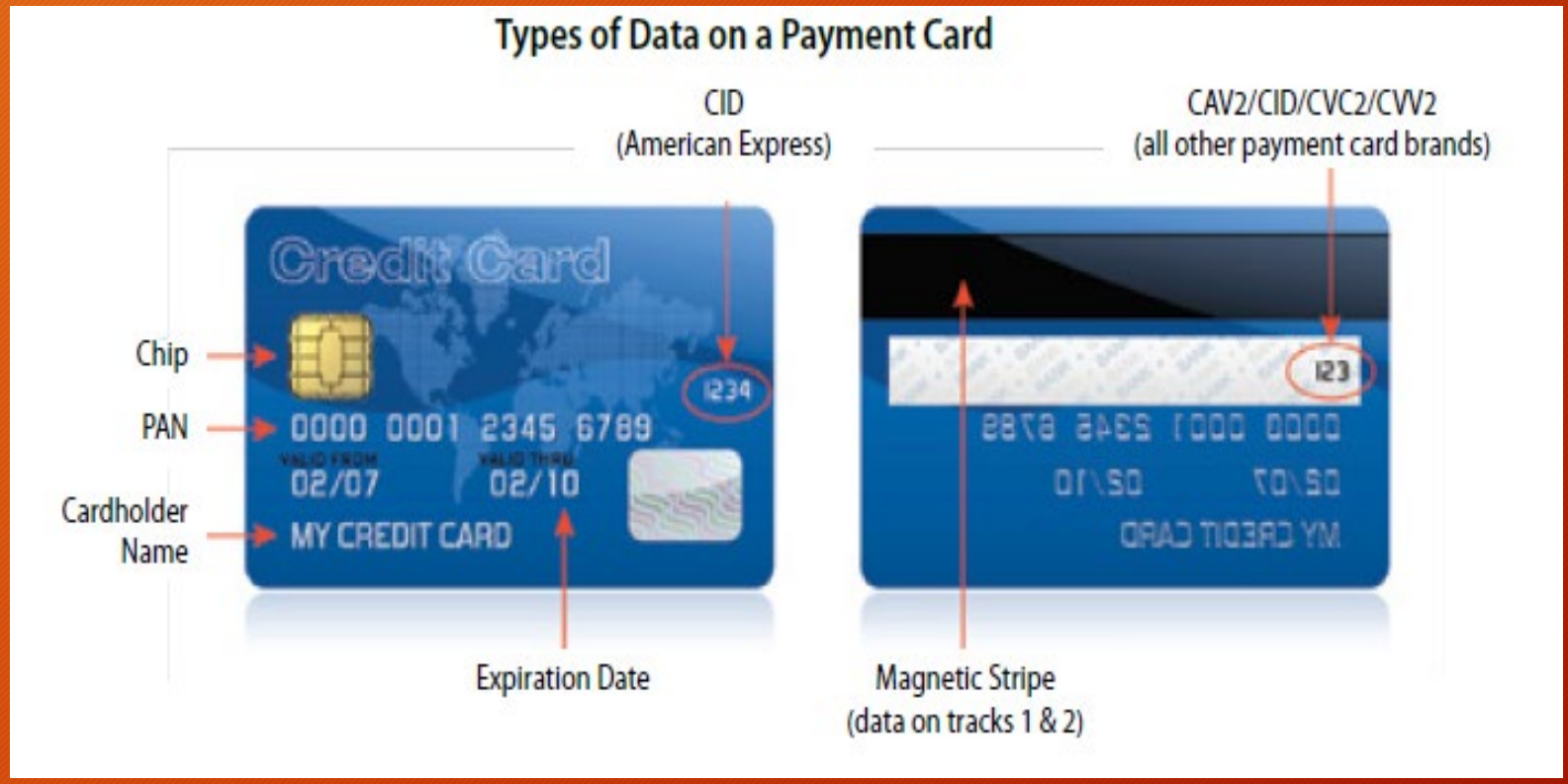
Office of the State Treasurer
State of Delaware

PCI-DSS Security Compliance Report

External Network Scan Remediation

What are the elements of a valid card?

Verify card elements and security features



What is the PCI DSS SCOPE?
These are within the PCI purview

- Scope include;
  - People
  - Processes
  - Technology
  - System components
  - Security-related devices connected to CHD components (firewalls, routers)
- Determining scope
  - Current inventory of systems and devices
  - Cardholder dataflow and network diagrams
  - Policies and procedures

PCI DSS – External Scan Result

Details of external scan implementation

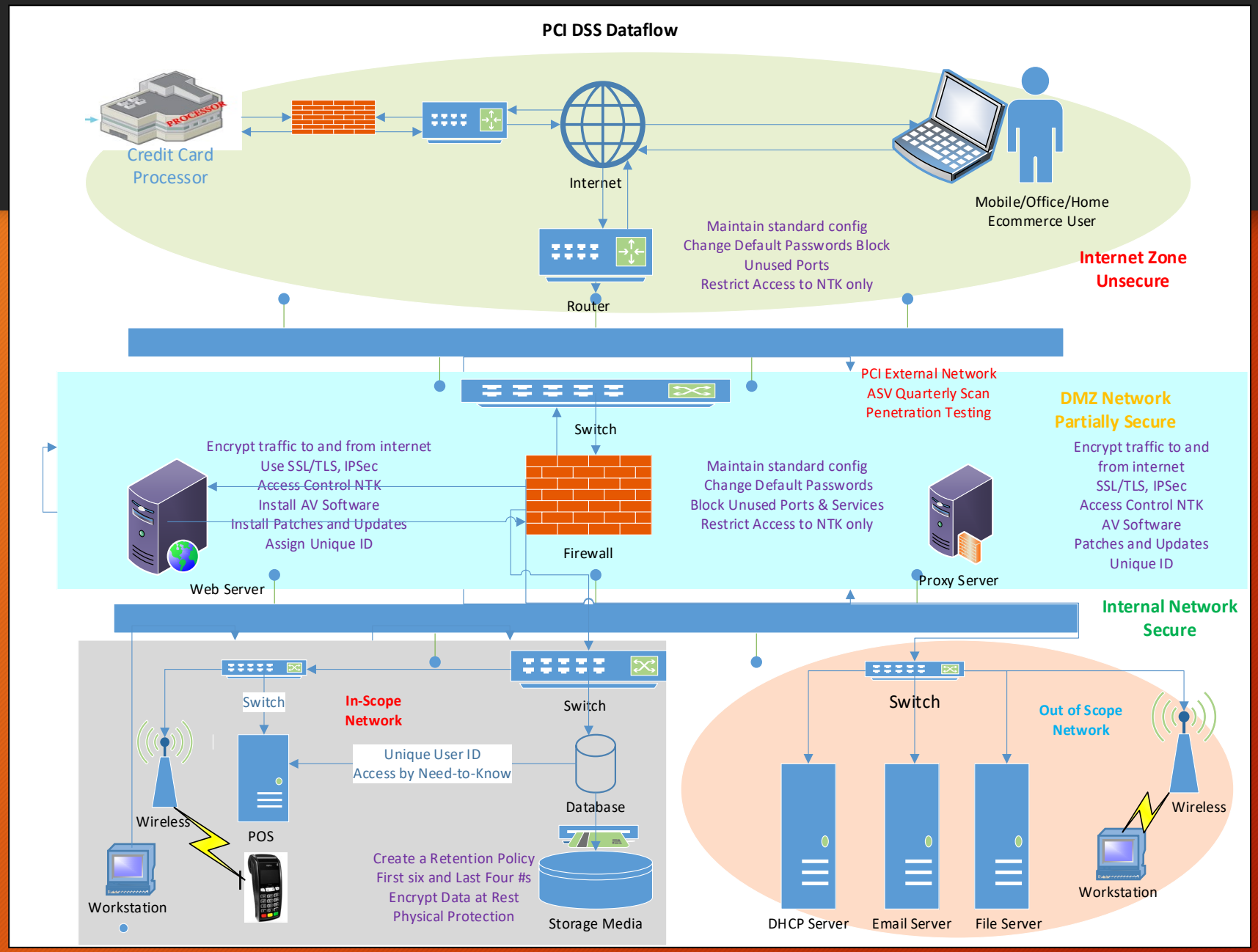
- Scan type: Full external scan
- Date of scan: 08/14/2019
- Expiration date: 11/12/2019
- Compliance status: Fail
- In scope components: 11 components (must be compliant)
- Out of scope components: 602 components (compliance not needed)
- Vulnerabilities: 164 (ranking as Low – Medium – High)
- Performed by: CampusGuard (ASV) contractor – mandated executor
- Frequency: Quarterly scans must be performed (mandated every 90 days)
- Remediation is now 65 percent complete

PCI DSS – External Scan Remediation Status

In scope components – Internet Facing

Device	Agency Name	Remediation Status
52.26.165.75	DHSS	Completed
52.43.37.58	DHSS	Completed
167.21.84.234	Department of Labor	Completed
167.21.9.98	Department of Education	Completed
167.21.84.18	Division of Revenue	Completed
167.21.84.126	Division of Finance	Completed
167.21.84.143	Division of Revenue	Completed
167.21.84.160	Division of Revenue	In progress
167.21.108.119	DHSS	In progress / partial
167.21.108.141	DHSS	In progress / partial
167.21.84.47	Department of Justice (Courts)	In progress

External zone (Internet) > Shared zone (DMZ) > Internal zone (CDE)



The Credit Card Transaction Process

- User is on the internet
- User searches your website address
- Router sends request to your DMZ Switch

Scenario One - DMZ web transactions

- DMZ switch sends request to firewall
- Firewall sends request to DMZ web server
- Web server collects data and send to credit card processor
- Credit card processor confirms with card issuer and validates with web server
- Web server accepts/deny customer transaction
- End

Scenario Two - Internal network process

- Scenario one takes place but at internal network rather than at web server
- Customer walks into the office and perform transaction

PCI DSS – Internal Network Scan Initiatives

Status – In Discovery Phase

- Reached out to all state agencies to advise on Compliance
- Requested information on internal IP addresses processing (CHD)
- Time is required for agencies to identify scope and discovery
- Received IPs from some agencies, a working process
- Install scan agents on all discovery components
- Perform PCI Compliance scans against components
- Rank vulnerabilities as Low – Medium – High
- Plan remediation actions against report findings (prioritized)
- Run quarterly internal PCI Compliance scans
- Remediate findings and Repeat process

Failure to comply could result in what?
Placement in a non-compliance status leading to:

- Payment brands may fine an acquiring bank $5,000 to 100,000 per month for PCI Compliance violations
- The bank will also most likely pass this fine along until it eventually hits the merchant
- Inability to accept credit cards for payments
- Termination of payment account or increased transaction fees
- Requirement to notify victims and pay replacement costs
- Reimburse fraudulent transactions
- Requirement to validate as a Level 1 merchant (QSA) – robust/expensive
- Damage to state reputation and public relations (PR)
- Loss of customer confidence to do business with the state or agency

PCI DSS consequences of a breach

- Direct Costs
  - Discovery and forensic analysis
  - Notification costs
  - Identity monitoring costs
  - Additional security measures
  - Lawsuits and fines
- Indirect Costs
  - Loss of productivity / distractions
  - Loss of customer confidence (declining business issues)
  - Reputation (PR)

US Data Breaches Leading to Exposure of Credit/Debit Card Details 2010 - 2018

- Equifax Hack: 5 Biggest Credit Card Data Breaches - A hack on credit bureau Equifax in September of 2017 exposed personal data of 143 million customers, including 209,000 credit card details.
- Capital One: 106 Million Customers Exposed
- Heartland Systems 2009: 160 Million Cards
- TJX Companies (TJX): 94 Million Cards
- TRW/Sears: 90 Million Cards
- The Home Depot (HD): 56 Million Cards

Summary
The PCI Program Initiative

- Discovery
  - Identify where all PCI data lives on the network (external and internal)
  - Determine PCI data network flow process (diagrams, transaction paths)
  - Secure PCI card data environment (CDE) – all devices connected
  - Perform quarterly PCI internal and external network scans
  - Develop a plan of action (POA) to remediate all vulnerability findings
  - Access, implement changes, update, and repeat process (continuous)
- PCI Policies and Procedures
  - Develop a comprehensive PCI master policy for the STATE
  - Master policy to include specific policy for all PCI deliverables
  - Develop Incident Response Plan against PCI security breach
  - Develop policy on PCI third-party engagements