Quarterly Business Officers Meeting

December 14, 2023

Today’s Agenda

- Credit Cards – Policy Update, CashNet & PCI Changes
  - Justin Evans, Viviana Wesley, Jonathan Pacheco
- Fringe Benefit Rates
  - Ted Welter
- Conflict of Interest
  - Debby Zumbach
- Resources on the Controller’s Office Website
  - Rachel McGuire

December 2023 Business Officers Meeting

Payment Card Industry Data Security Standards (PCI DSS)

Thursday, December 14, 2023

About the Presenters

Justin Evans

- Senior IT Security Analyst, University of Iowa Information Security and Policy Office
- University of Iowa Tippie College of Business: Executive MBA 2022
- Payment Card Industry Professional (PCIP): 2020
- American Academy of Professional Coders (HIPAA & Revenue Cycle Management): Certified Professional Coder and Instructor (CPC, CPC-I)

About the Presenters

Viviana Wesley

- Principal Consultant with HALOCK Security Labs
- CISM, PCI QSA, ISO 27001 Auditor
- HALOCK's PCI DSS Subject Matter Expert and Solutions Architect
- 22+ years of practical experience within Information Technology
- 13+ years specializing in Information Security
- University of Northern Iowa – Bachelor of Arts in Computer Science
- Worked at the University or Northern Iowa for 5 years

Agenda

Future

- Increased security threats
- Stronger PCI DSS 4.0 requirements

History

- Merchant choice and convenience
- 2 recent examples of fraud

Recommendations

- SAQ A (card-not-present wholly outsourced eCommerce)
- SAQ P2PE (card present)

Opportunities

- Partner with Treasury and ISPO to implement secure business practices
- Present reasonable and defensible security posture to regulators

IOWA

What is PCI DSS?

- Credit Card Brands
- Payment Card Industry Security Standards Council (PCI SSC)
- Payment Card Industry Data Securities Standards (PCI DSS)

The PCI SSC is an independent industry standards body providing oversight of the development and management of Payment Card Industry Data Security Standards on a global basis.

The PCI SSC provides training for several different qualifications and programs.

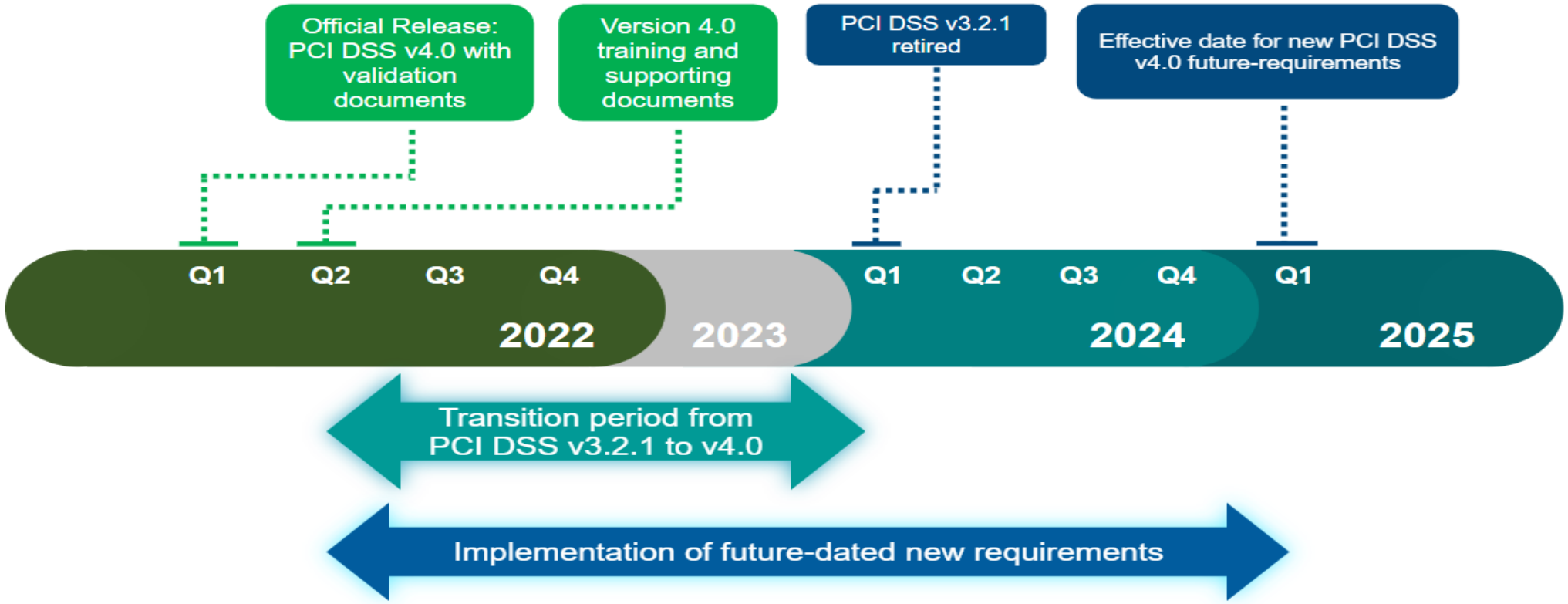
PCI SSC founding payment brands include:

- American Express
- Discover Financial
- JCB International
- MasterCard
- Visa, Inc.

IOWA

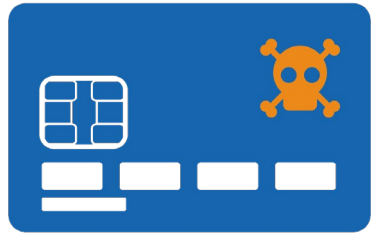
PCI DSS v4.0 Transition Timeline

Transition Timeline



IOWA

We've Been Hacked!



- **The Incident Report:** "Our credit card payment system is hacked."
- **The Merchant:** SAQ A-EP via direct post
- **The Attack:** High velocity credit card authorization testing
  - Game of Whack-a-mole making fraud filter adjustments to hosted payment page
- **The Solution:**
  - Short-term - CAPTCHA plus payment and sales price alignment
  - Long-term – Wholly outsourced eCommerce TPSP (Third-party Service Provider)

We've Been Hacked Episode 2: Attack of the Clones!

- **The Merchant:** ISPO we have a problem
- **The Midnight Refund:** Who dunnit?
- **The Attack:** Cloned PoS terminal made remote refund to unknown card
- **The Merchant Bank:** We need to talk!
  - Cloned devices known issue, but still being sold
- **The Solution:** P2PE (Point to Point Encryption) is the standard for in-person payment card acceptance

Why Reduce Scope?

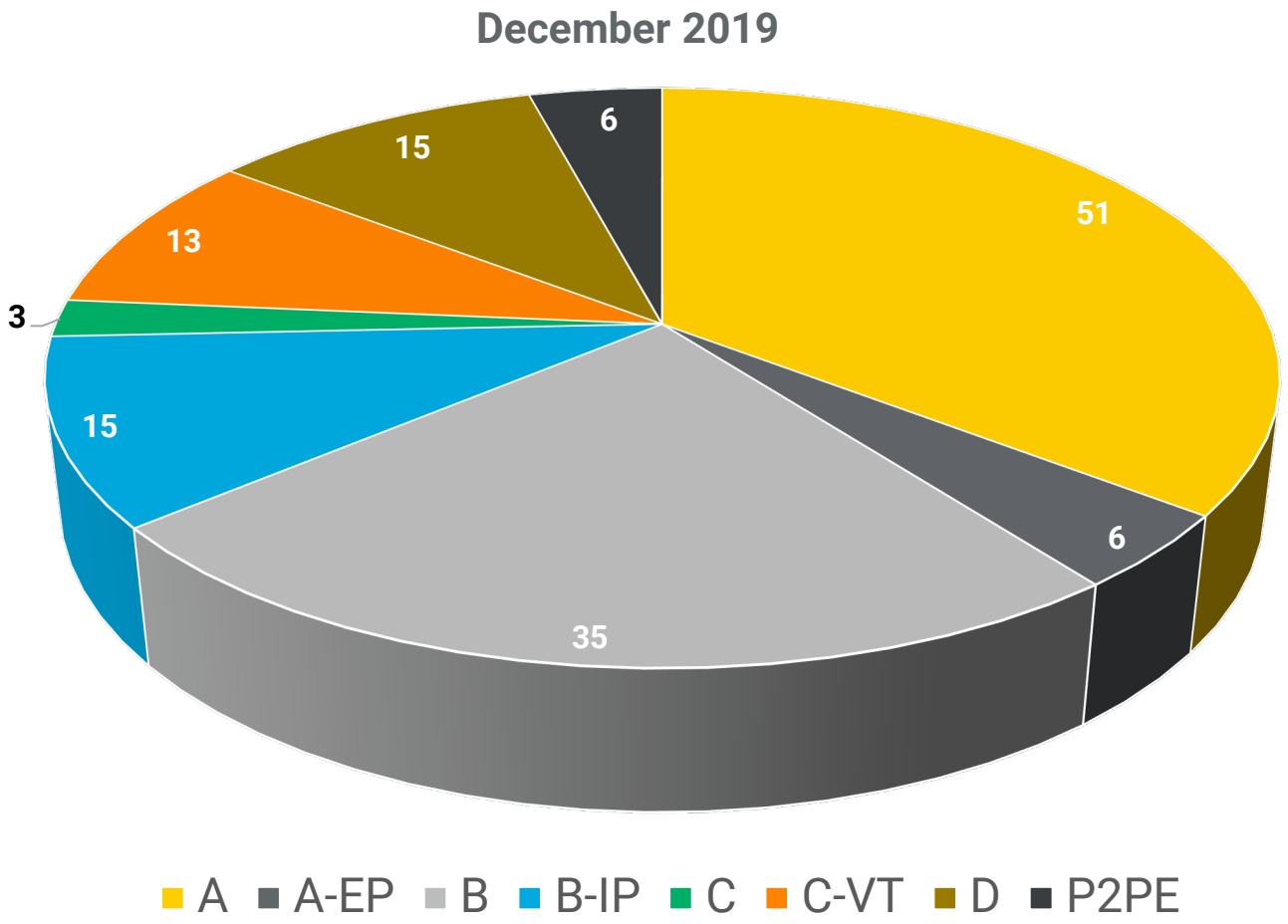
3-Year consolidation effort has reduced risk and increased efficiency

- **Wholly Outsourced eCommerce:** Dozens of SAQ A merchants processing under a single merchant ID
- **Reduced** merchant compliance reporting
- **P2PE:** Standard card present solution as old devices reach end-of-life and merchant contracts are up for renewal
- **PCI-focused resources freed** to meet higher value security and privacy needs

How it Started: December 2019

Total Number of Reporting Merchants: 144

- **SAQ A:** 51
- **SAQ A-EP:** 6
- **SAQ B:** 35
- **SAQ B-IP:** 15
- **SAQ C:** 3
- **SAQ C-VT:** 13
- **SAQ D:** 15
- **SAQ P2PE:** 6

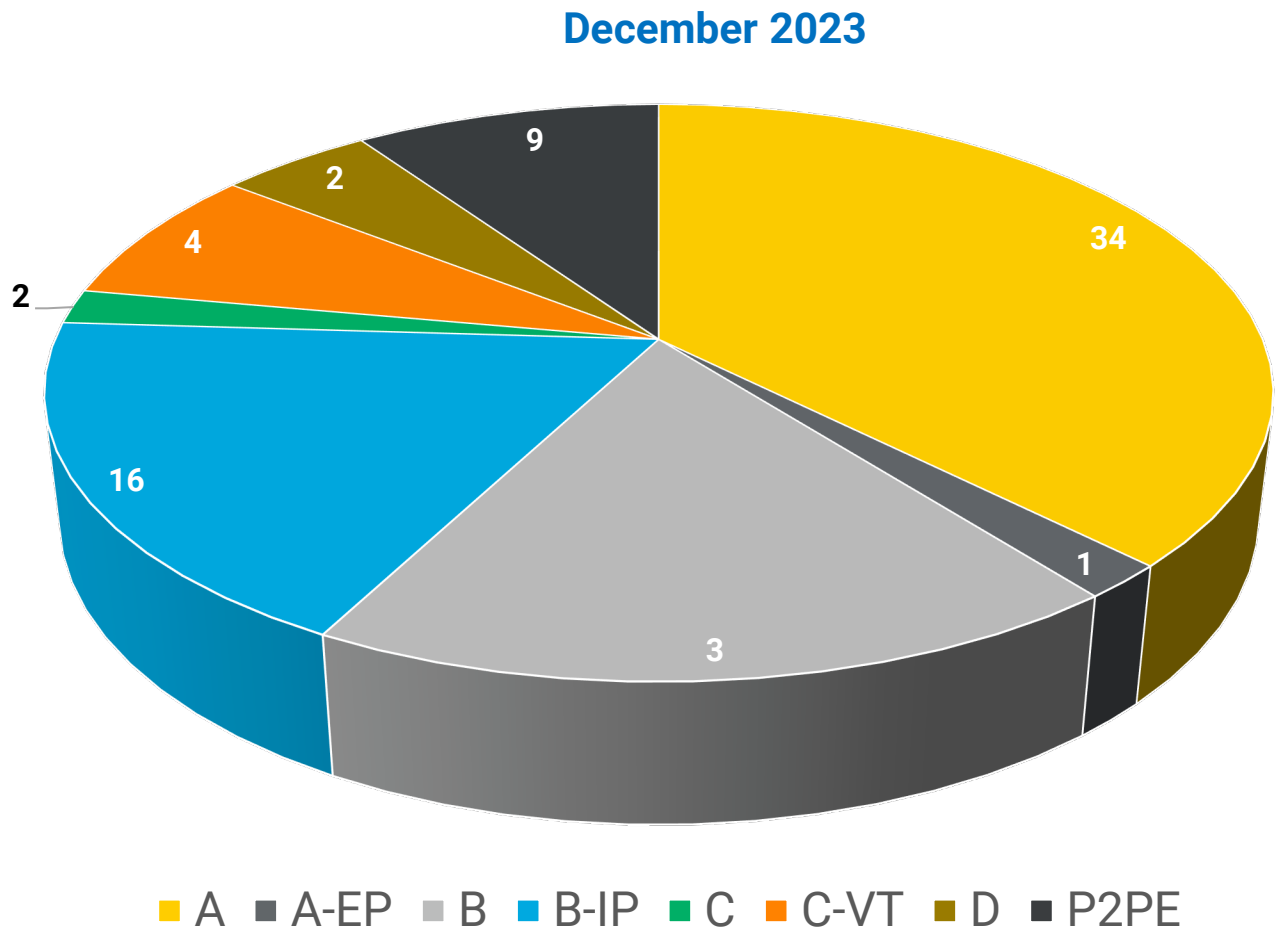


IOWA

How it's Going: December 2023

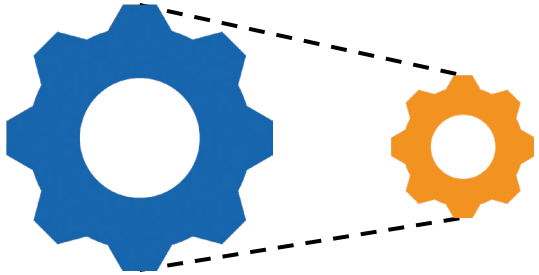
Total Number of Reporting Merchants: 144 → 71

- **SAQ A:** 51 → 34
- **SAQ A-EP:** 6 → 1
- **SAQ B:** 35 → 3
- **SAQ B-IP:** 15 → 16
- **SAQ C:** 3 → 2
- **SAQ C-VT:** 13→ 4
- **SAQ D:** 15 → 2
- **SAQ P2PE:** 6 → 9



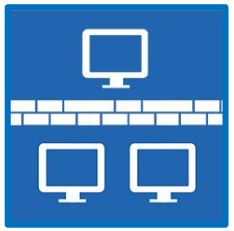
IOWA

ISPO Recommendations and Why



- **Based on discussions with our PCI QSA**
  - **Reduce PCI DSS compliance Scope**
- **Why? It Reduces:**
  - Risk
  - Remediation time
  - Remediation cost
  - The resource needs for remediation and ongoing compliance maintenance
- **After a breach, card brands strongly recommend using validated P2PE solutions.**

PCI Scope Reduction Options



Network Segmentation

- Not a PCI DSS requirement but can be used to reduce scope through isolation. Often the most time consuming to setup and maintain.

Outsource to PCI DSS-compliant Service Providers

- Variety of options from payment handling to managed security service providers.

Use P2PE

- Remove your systems and networks from handling sensitive data for any card present or card-not-present processing that is performed by an employee.

Change Business Processes

- People can update processes to remove full PAN when not required.

IOWA

Point-to-Point Encryption (P2PE)

- Encrypted cardholder data may be deemed out of scope if it has been validated that the entity that possesses the data **does not have the means to decrypt it.**
- Requires compatible card swipe devices and a payment processor that provides the end-to-end encryption service.
- *If implemented correctly, can render most PCI requirements non-applicable for much of the environment.*
- Only PCI SSC validated P2PE solutions provide full scope reduction (unless the solution can meet acquirer risk acceptance requirements).

ISPO Recommendations

- Still always have **PCI Network Topology** and **Cardholder Data Flow diagrams** to explain how payment processing is handled.
- **If outsourced, *explicitly* explain** how the merchant organization does not have access to cardholder data.
- **When this documentation exists, witnessed Common Point of Purchase (CPP) investigations quickly close**, as the focus shifts to solution providers.

ISPO Recommendations

- Familiarize yourself with the Treasury Merchant Services – Credit Card Policy and Security Standards policy located here: https://treasury.fo.uiowa.edu/sites/treasury.fo.uiowa.edu/files/wysiwyg_uploads/merchant_services_-_credit_card_policy_and_security_standards_web.pdf

- Submit a Security Review for any potential new technology solutions or outsourced providers – Please work with local IT support to submit the Security Review. https://itsecurity.uiowa.edu/security-review-frequently-asked-questions

IOWA

ISPO Recommendation: Security Review Form

Data Classification & Integration

UI Data Classification Policy can be found here: https://itsecurity.uiowa.edu/institutional-data

Compliance What are the regulatory/contract/grant controls to which the system/ application must comply? (Please check all that apply):

Optional

- [ ] HIPAA
- [ ] FERPA
- [ ] PCI-DSS
- [ ] NIST SP 800-171/DFARS
- [ ] FDA
- [ ] GLBA
- [ ] ITAR/EAR
- [ ] Other

IOWA

ISPO PCI Strategies

- Card present merchants should use PCI SSC P2PE Validated solutions
- Card-not-present merchants should outsource to Transact eMarket (CashNet) when possible
- Progressively consolidate card acceptance solutions
- Learn about PCI DSS 4.0 requirement changes coming in 2024 and 2025 and prepare with individual stakeholders as needed

Questions?

UI Treasury Operations
UI Information Security and Policy Office
HALOCK Security Labs

Thank you!

→ uiowa.edu

Transact Cashnet Storefronts

- 270 storefronts
- 19,500 sales
- $2,400,000 revenue

- New Cashnet Storefront Request Application
- Contact: treasury-creditcards@uiowa.edu or jonathan-pacheco@uiowa.edu

IOWA

Fringe Benefit Rates

Ted Welter, Assistant Controller

Dec. 2023 Quarterly Business Officer Meeting

FY25 Fringe Rates

Rate Pool	FY24	SUBMITTED FY25	Change
Clinical Faculty	25.6%	24.7%	(0.9%)
Non-Clinical Faculty	31.2%	31.4%	0.2%
P&S	41.2%	40.5%	(0.7%)
SEIU	42.4%	42.5%	0.1%
Merit	53.7%	54.0%	0.3%
House Staff	25.5%	26.0%	0.5%
Grad Asst/Post Docs	20.3%	19.7%	(0.6%)
Fellowships	9.8%	9.6%	(0.2%)
Temporary	11.8%	11.8%	0.0%
Student	7.0%	7.2%	0.2%
Miscellaneous	5.3%	4.7%	(0.6%)

Clinical Faculty Rate Calculation

	FY23 Actual	
Salary Base (A)	298,104,251	
Fixed Rate	24.4%	
Benefits Recovered	72,737,437	
Benefit Costs (B)	72,254,484	24.2%
Over (Under) Recovery	482,953	
Carryforward from FY21	(1,849,269)	
Carryforward to FY25 (C)	(1,366,316)	
Submitted Rate (B-C)/A	24.7%	

IOWA

Three-Year Actual Rate History

Rate Pool	FY21	FY22	FY23	SUBMITTED FY25
Clinical Faculty	23.7%	24.0%	24.2%	24.7%
Non-Clinical Faculty	30.6%	30.6%	31.0%	31.4%
P&S	40.1%	40.0%	40.2%	40.5%
SEIU	42.4%	42.4%	42.3%	42.5%
Merit	54.5%	54.4%	54.1%	54.0%
House Staff	25.4%	25.5%	25.7%	26.0%
Grad Asst/Post Docs	19.8%	20.0%	19.8%	19.7%
Fellowships	10.8%	10.6%	10.2%	9.6%
Temporary	11.7%	11.6%	11.8%	11.8%
Student	7.5%	7.1%	7.6%	7.2%
Miscellaneous	5.0%	5.0%	5.0%	4.7%

Projected Fringe Rates

- Update projected starting in March
  - FY26 using calculation
  - FY27 actual rate

- Available on website and a table in the data warehouse

Resources on the Controller's Office Website

- Use of certain institutional accounts (Iaccts) for acquisitions of equipment, software and leases
  - https://cam.fo.uiowa.edu/institutional-accounts-iaccts-acquisitions-equipment-software-and-leases

Thank you

→ uiowa.edu

IOWA