GETTING THE MOST OUT OF YOUR COMPLIANCE PROGRAM

State of North Carolina Office of State Controller

Coalfire Webinar Series

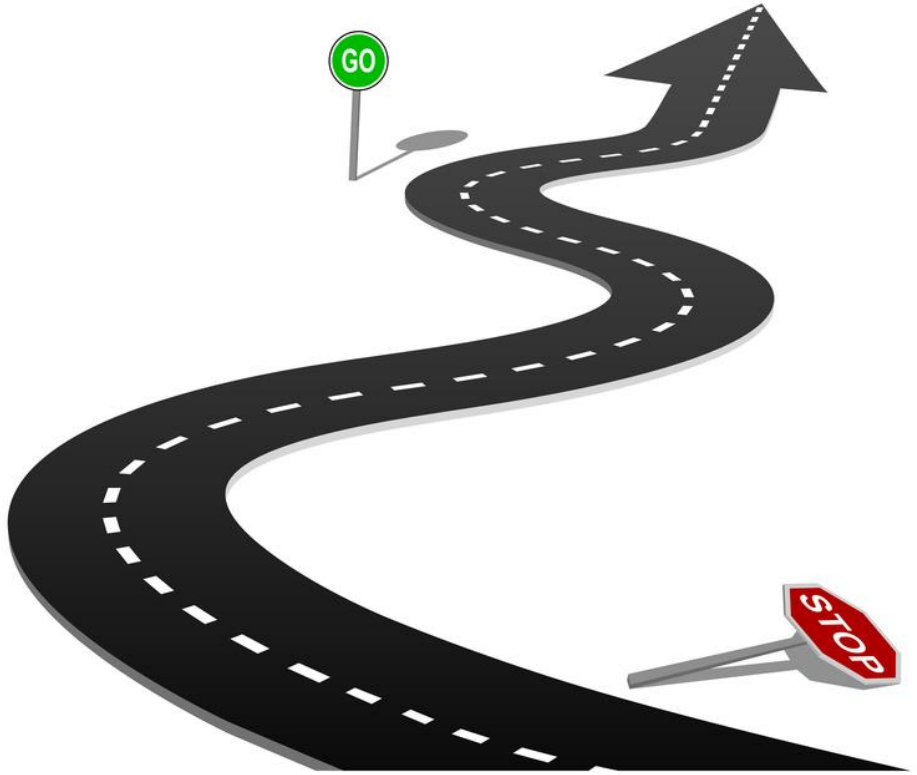
March 22, 2018

Presenter: Joseph D. Tinucci, QSA, CISSP

WHERE WE ARE HEADED

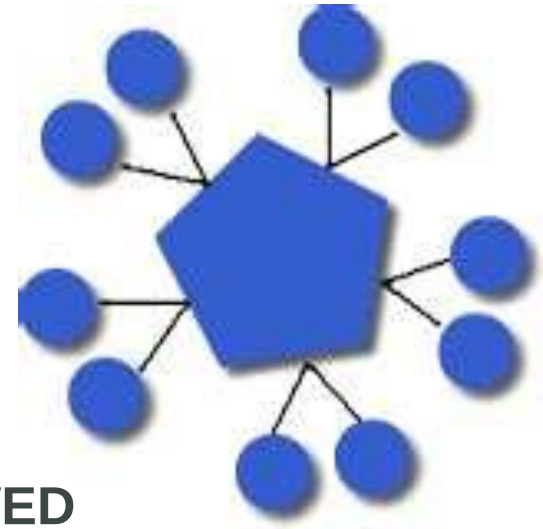
Characteristics of a Strong PCI DSS Compliance Program

- Centrally Coordinated and Managed
- Knowing Where Your (Cardholder) Data Is
- Partnering Between Technical and Business Sides
- Supporting Your Business Needs Compliantly
- Implementing Best Business Practices
- Looking at More Than Just Payment Cards
- Getting the Technology Right
- Looking to the Future



COALFIRE

CENTRALLY COORDINATED AND MANAGED



Give your Acquirer confidence

- Use a Project Management approach
- Distribute information security policy to departments / merchants
  - Help them customize for PCI DSS
  - Ensure they have **WRITTEN** procedures in place and **FOLLOWED**
- More efficient and consistent training
- Prevent procurement disasters
  - Get them to understand payments and risk **BEFORE** they sign the contract
  - Helpful to ensure that all vendors start compliant and stay compliant
- Reduces unmanaged risk
  - Know where and how payments are being processed
  - Who is accepting telephone payments? Mobile payments?

CALFIRE

COALFIRE CAN PROVIDE

- Policy development advisory service
- Ad hoc and customized training / workshops
- Risk advisory

COALFIRE

KNOW WHERE YOUR (CARDHOLDER) DATA IS

And what your organizational parts do with it

- Inventory of merchants
- Inventory of merchant ecommerce sites
  - Who is hosting the site?
  - Who is building / maintaining the site?
- Telephone payments being processed
  - Cardholder data being written down on paper, handled appropriately?
  - Using Voice over IP (VoIP) networks?
  - Conversations being recorded?
- Stored Cardholder Data
  - Do they have a legitimate business need to store CHD?
  - Are they properly protecting it? How are they encrypting it?

COALFIRE CAN PROVIDE

- Needs Assessment projects (who does what how)
- Merchant education webinars / workshops
- Self Assessment (SAQ) Advisory / Facilitation
- Sensitive data / CHD search and destroy
- VoIP architecture and security consulting

COALFIRE

PARTNERSHIP BETWEEN TECHNICAL AND BUSINESS SIDES

Neither side can do this alone

- Manage the bank / OSC relationship
- Pre-qualify both the merchant business case for accepting payment cards as well as the technical processing methods for PCI compliance
- Prepare and propagate policies and procedures to merchants
- Guide the merchants to implement best practices – both business and technical
- Manage vendors (central contract approval, negotiation, PCI compliance)
- Prequalify the technology to be used for payments
- Document the centrally-provided IT infrastructure

CALFIRE

COALFIRE CAN PROVIDE

- Policy consultation, analysis and review
- Network architecture advice
- Assistance with RFP technical evaluation

COALFIRE

SUPPORT YOUR MERCHANTS' BUSINESS NEEDS COMPLIANTLY

Keep the business needs in mind while evaluating processing methods

- Require a needs analysis / business case for new merchant accounts, new processing methods
  - Prepare a compliance pre-analysis before putting new merchants into your portfolio
  - Consider compliant alternatives if original method might not be compliant or meet the organization's requirements (no storage of CHD, etc.)
- Prepare a risk assessment of current practices, processes
- Evaluate ecommerce sites for vulnerabilities, processing methods
  - SAQ A or SAQ A-EP?
- Implement both best business and technology practices

COALFIRE CAN PROVIDE

- Assessment of unlisted End-to-End Encryption (E2EE) solutions for reduced-scope compliance
  - Even though not a listed P2PE solution, might qualify for fewer controls than an SAQ C or D
- Assistance with risk assessments
- PCI Advisory services

COALFIRE

IMPLEMENT BEST BUSINESS PRACTICES

People are as important as the best of technology

- Best business practices reduce risk
- “Security as Business as Usual”
  - Move appropriate compliance tasks from annually to more frequently (POI device inspection, etc.)
  - Distribute compliance / review tasks among several staff members
  - Ongoing security training rather than once each year
- Ensure strong internal controls
  - No reason to handle cards carefully and be sloppy with cash
- Handle cardholder/sensitive data on paper properly
  - Always use “the form”

- Always ask “Can we do this better or more effectively?”

COALFIRE

COALFIRE CAN PROVIDE

- Business process advisory services
- SOC audits
- HIPAA advisory services
- FedRAMP consulting / certification

COALFIRE

LOOK AT MORE THAN JUST PAYMENT CARDS

PCI Compliance does not exist in a vacuum…

- Integrate payment processing as part of cashiering
  - Treat other forms of payment as carefully as you do cards
- Implement a “Compliance Mindset” and awareness among staff
- What other compliance regimens apply to you ?
  - FERPA, HIPAA, ITAR, NIST 800-171, FISMA
  - Research data, health data, privacy laws, breach disclosure requirements
  - GDPR – European Union General Data Protection Regulation
  - General risk assessment

CALFIRE

COALFIRE CAN PROVIDE

- GDPR, HIPAA, FISMA, NIST 800-171 consulting
- Risk advisory / assessment services
- Incident Response
  - Testing
  - Forensics
  - Advisory
- Network penetration testing
- “Red Team” services

COALFIRE

GET THE TECHNOLOGY RIGHT

Technology helps support your crack staff

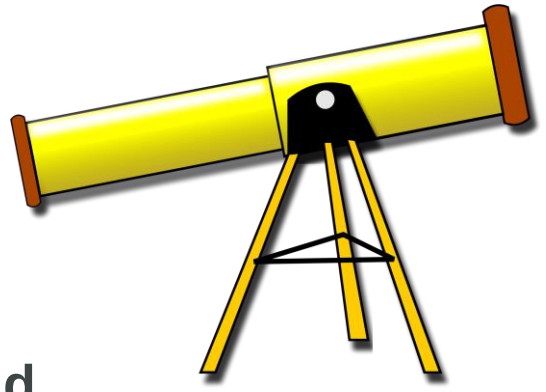
- Technology can greatly simplify risk and compliance
  - P2PE, E2EE (unlisted P2PE), EMV cards
  - 3D Secure (a/k/a “Verified by Visa”) for ecommerce
  - Mobile payments (upcoming “PIN on Glass” standard)
  - Proposed Secure Payments Software Development Framework
  - Moving to the “cloud”
- Technology can be very complex
  - Moving to the cloud
  - Taking payments over VoIP phone lines
  - Recording payment conversations
  - Shortage of good technology skills
  - Ransomware, Internet of Things (IoT) Distributed Denial of Service (DDOS)

COALFIRE CAN PROVIDE

- Secure cloud deployment guidance, advisory
- IoT security architecture advisory
- VoIP consulting
- Vulnerability scanning (internal, ASV external)
- Penetration testing
- Log management and analysis (Splunk)
- Firewall tuning (Palo Alto)
- Web application penetration testing

COALFIRE

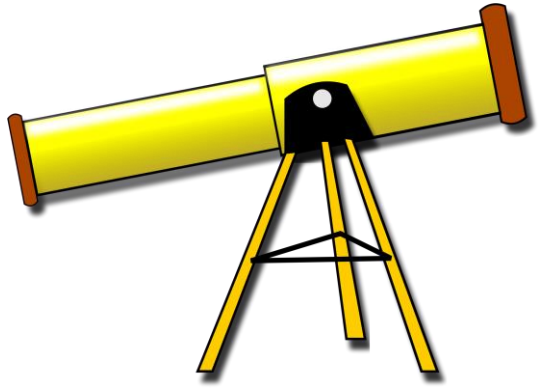
LOOK TO THE FUTURE 1



Position your organization for what is coming down the road

- Reduce scope / risk as much as possible
  - Implement P2PE + EMV solutions for all card-present, mail order / telephone order (MOTO) payments
  - Implement 3D Secure for online payments
  - When available, implement SPoC (Software-Based PIN Entry on COTS) (PIN on Glass)
  - Only use PCI-compliant service providers
- Review current business practices for improvement
- Implement a risk assessment / risk review process

LOOK TO THE FUTURE 2



- Train! Train! Train!
  - Increase staff technical training to offset security skill shortage
  - Educate your users on current responsibilities, upcoming regulatory changes
  - Educate your users about phishing, ransomware, email and web best practices
  - Train your replacement
- Review ecommerce practices / websites
  - Apply professional development practices to all web sites
  - Jettison unsecure web technologies (Flash, Shockwave, outdated CMSs)
  - HTTPS everywhere

CALFIRE

LOOK TO THE FUTURE 3 - VOIP

Pay attention if you take payments by telephone

- The PCI Council has specifically stated that Voice over IP (VoIP) telephony systems are in scope if used to accept payments
  - **FAQ 1153 – *Is VoIP in scope for PCI DSS*?**
- If using VoIP for merchants and/or call centers, then you must examine the VoIP system security as part of your self-assessment
- Most VoIP systems have some level of default security (if turned on)
- Consult with your system implementer / telephony consultant regarding the system's current and potential security features
  - Ask them if the system could pass an SAQ D
  - VoIP security is simply network security
  - Get expert help if you need it

COALFIRE

COALFIRE CAN PROVIDE

- Blog postings at https://www.coalfire.com/The-Coalfire-Blog
- Multiple resources at https://www.coalfire.com/Resources
  - Case Studies
  - White Papers
  - Webinars
  - Videos
  - Data Sheets
- Planning / Roadmap creation assistance

COALFIRE

YOUR COALFIRE TEAM

We are here to support you

- **Derrick Roche, Account Manager**
  - Derrick.Roche@coalfire.com
- **Jon Bonham, Principal**
  - Jon.Bonham@coalfire.com
- **Steve Durham, Associate**
  - Steven.Durham@coalfire.com
- **Joe Tinucci, Senior Consultant**
  - Joseph.Tinucci@coalfire.com
- **Marvin Reader, Managing Director**
  - Marvin.Reader@coalfire.com

COALFIRE

QUESTIONS?

COALFIRE