

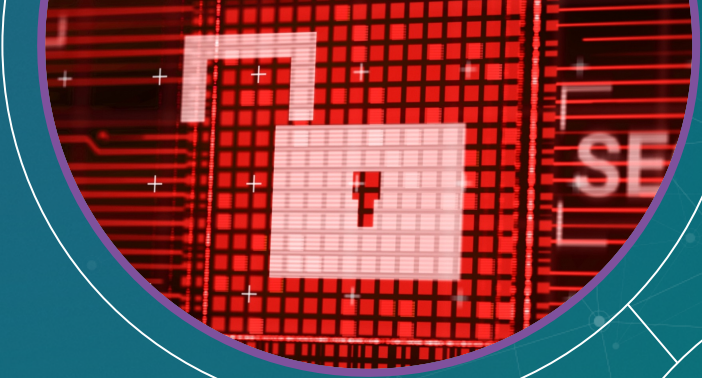
Preventing Data Breaches Panel Discussion

Brandy Cumberland, Director, Program Quality, PCI Security Standards Council

Chris Hague, Divisional Head – Technical Services (DFIR, TIG, SOC), Foregenix, Inc.

Kevin Bong, Cybersecurity Director, Sikich, LLP

Héctor Guillermo Martínez, President, GM Sectec



The background features a dark teal color with a complex pattern of glowing blue and red circuit traces. A large, semi-transparent magnifying glass is positioned on the left side, its lens centered over a specific area of the circuit board. Inside the lens, a bright yellow and orange light flare emanates from a point, highlighting a section of the circuit. The overall aesthetic is high-tech and digital.

PCI Forensic Investigators (PFIs)



PFI Final Report: Appendix A



Payment Card Industry (PCI) Data Security Standard Final PFI Report

Template for Final PFI Report

Version 3.2

July 2021



Appendix A PCI DSS Overview

To assist in identifying where breached (or potentially breached) entities failed to fully adhere to the PCI DSS, PFI Companies must submit a copy of *Appendix A* directly to PCI SSC via the Portal.

Note: When completing this section do not include any information that identifies the Entity Under Investigation.

QSA Employee who performed the technical review in accordance with the PFI Qualification Requirements:

QSA Employee name:

QSA Employee phone number:

QSA Employee e-mail address:

A.1 PCI DSS Summary

Type of business entity / payment channels	<input type="checkbox"/> Merchant: Card present; face-to-face (e.g., brick and mortar)	<input type="checkbox"/> Acquirer	<input type="checkbox"/> Third-party service provider (web hosting; co-location; integrator reseller) Identify type of service provider:
	<input type="checkbox"/> Merchant: Card not present <input type="checkbox"/> e-comm <input type="checkbox"/> MOTO	<input type="checkbox"/> Acquirer processor	<input type="checkbox"/> Encryption Support Organization (ESO)
	<input type="checkbox"/> Prepaid issuer	<input type="checkbox"/> Issuer processor	<input type="checkbox"/> Payment application vendor
	<input type="checkbox"/> Issuer	<input type="checkbox"/> ATM processor	<input type="checkbox"/> Payment application reseller

Was there conclusive evidence of a breach? Yes No

Summary statement for findings, including factors that caused or contributed to the breach. (For example, memory-scraping malware, remote access, SQL injection, etc.)

Was a PCI DSS Assessment performed prior to the incident under investigation? Yes No

Learning from Experience



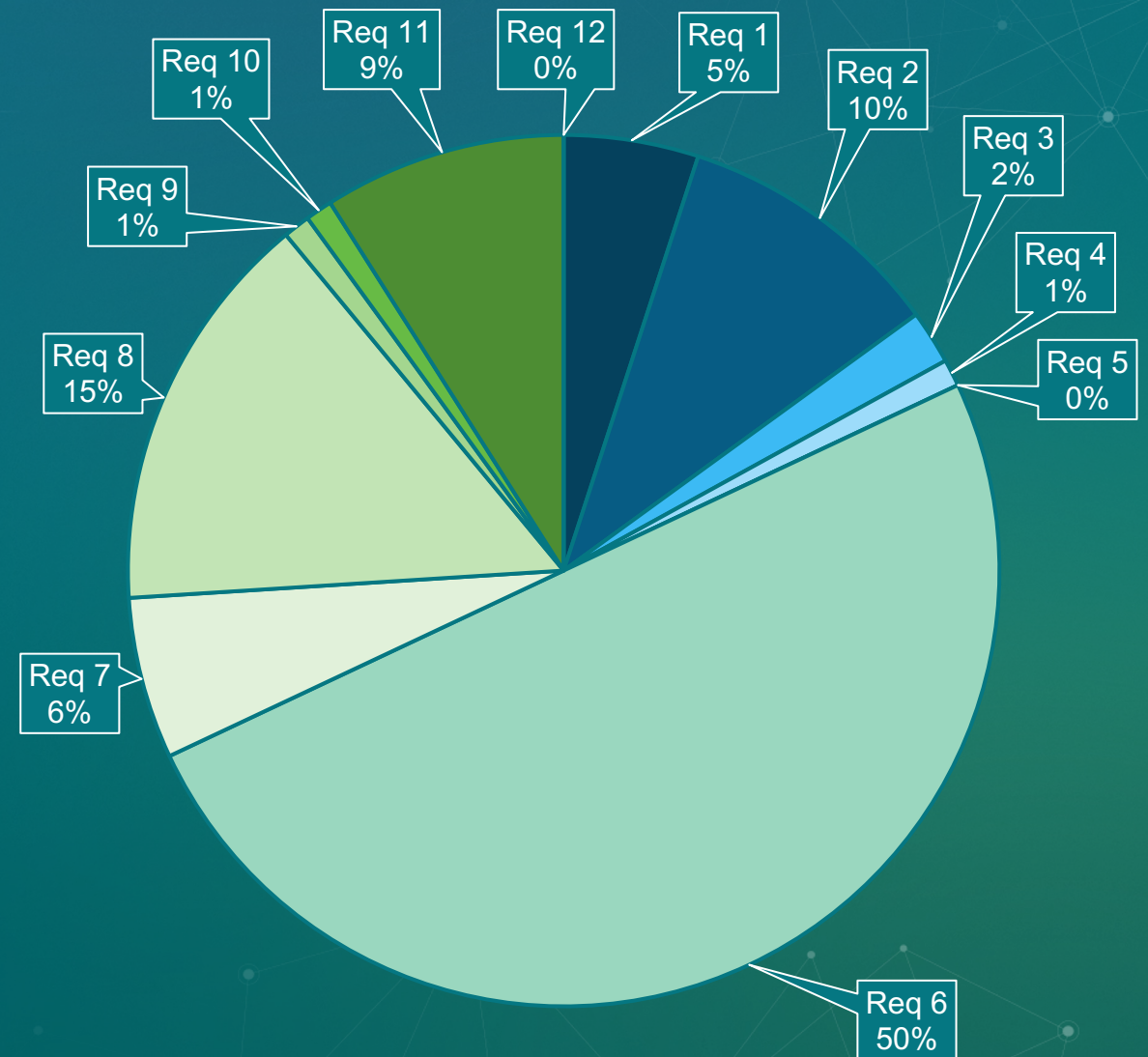
Results remain fairly consistent year-to-year

Failures at these Requirements are most often cited as causing and/or contributing to overall breach:

Requirement 6

Requirement 8

Requirement 11



Requirement 6: Develop and maintain secure systems and applications



Requirement 8: Identify and authenticate access to system components



Requirement 11: Regularly test security systems and processes



Final Insights from the PFIs

