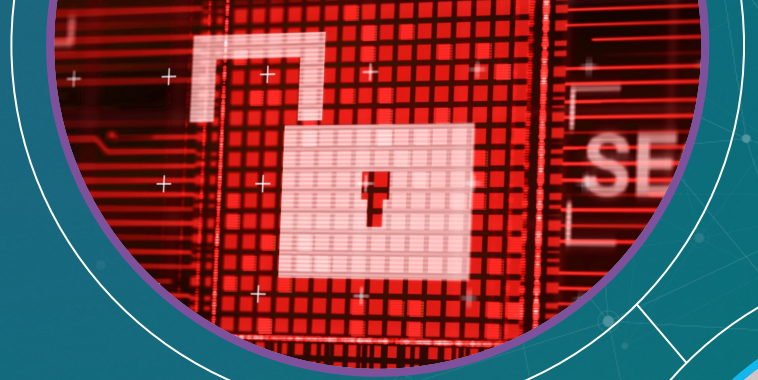
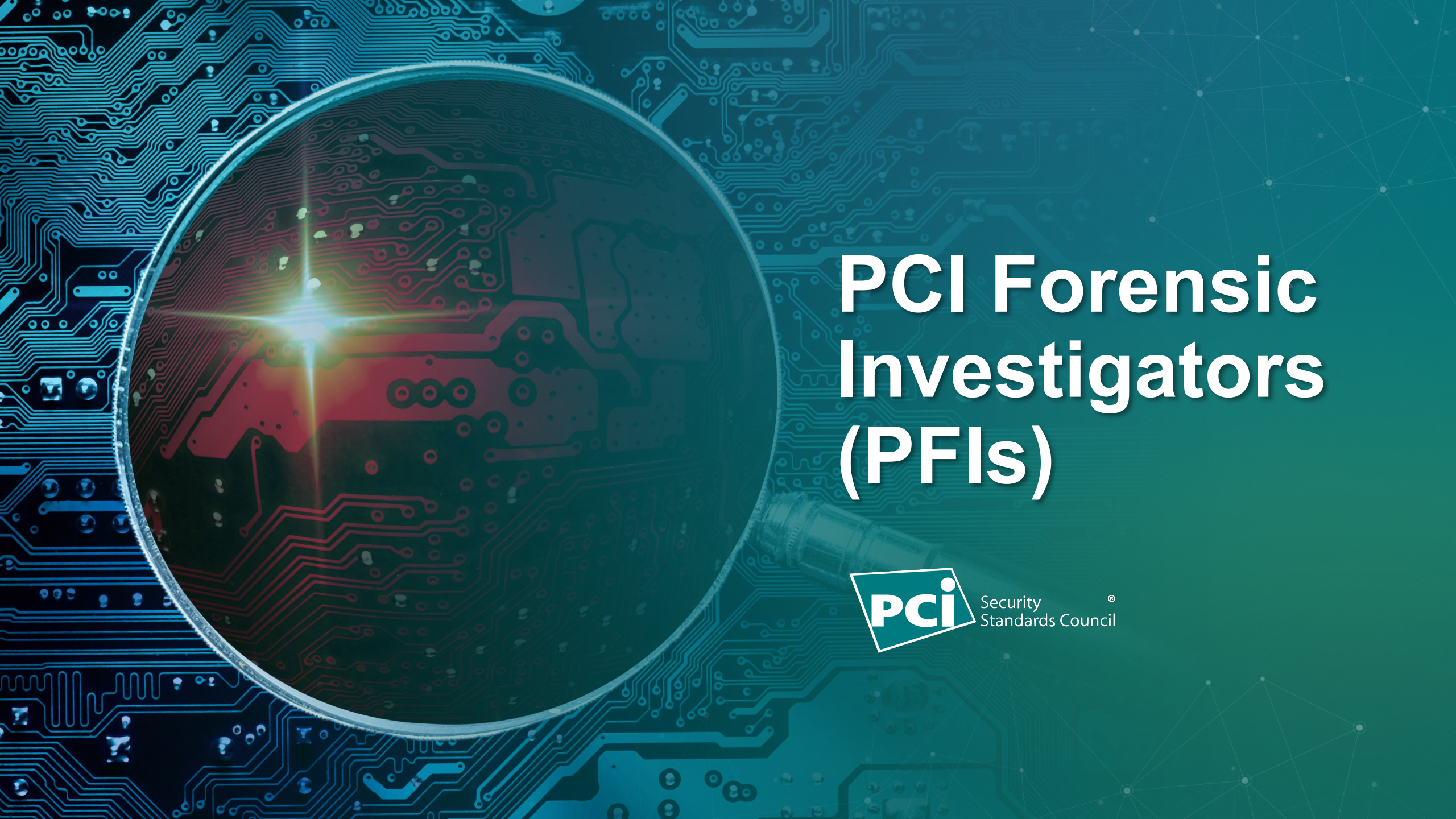
Preventing Data Breaches Panel Discussion

Moderator: Brandy Cumberland, Director, Program Quality, PCI Security Standards Council
Panelists:
Christopher Hague, Division Head – Technical Services, Cyber Security Consulting,Foregenix, Inc.
Christopher Novak - Managing Director, Cyber Security Consulting, Verizon
Benn Morris, Managing Director, 3B Data Security

PCI Security Standards Council®

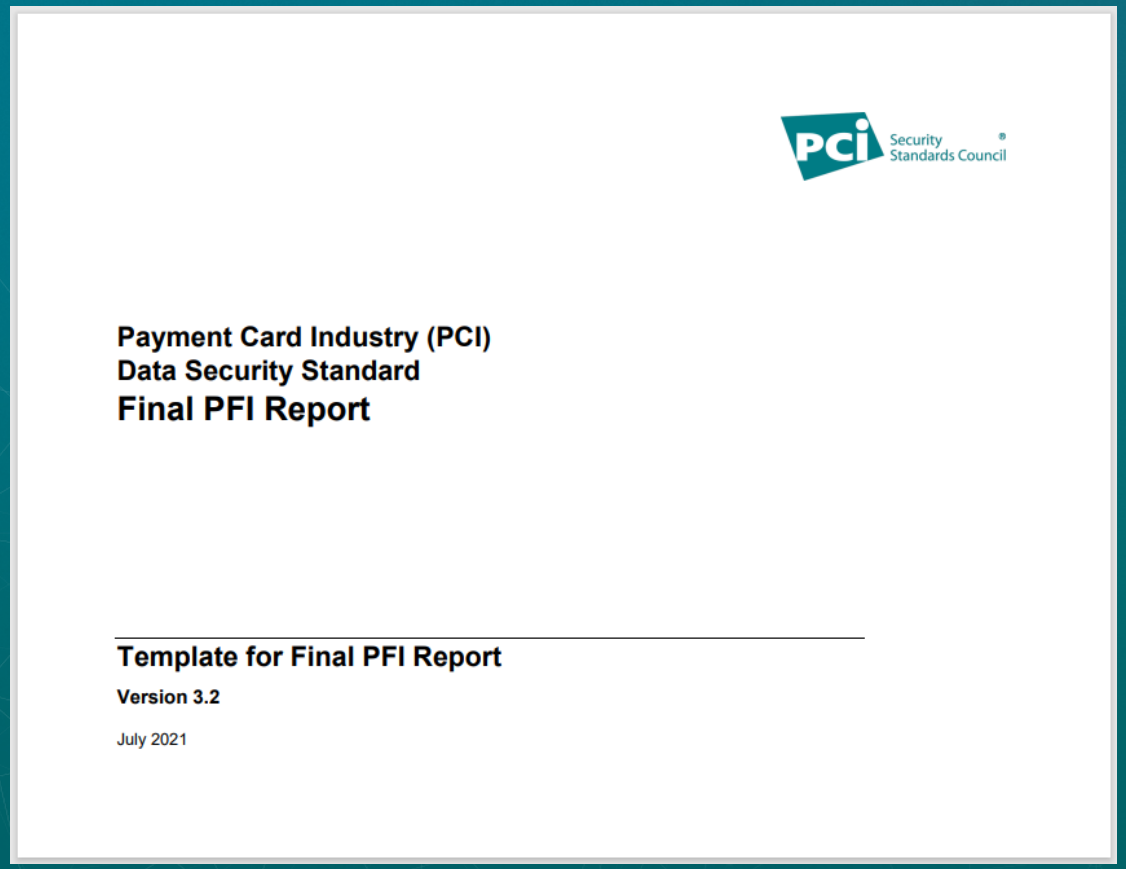




PCI Forensic Investigators (PFIs)

PCI Security Standards Council®

PFI Final Report: Appendix A

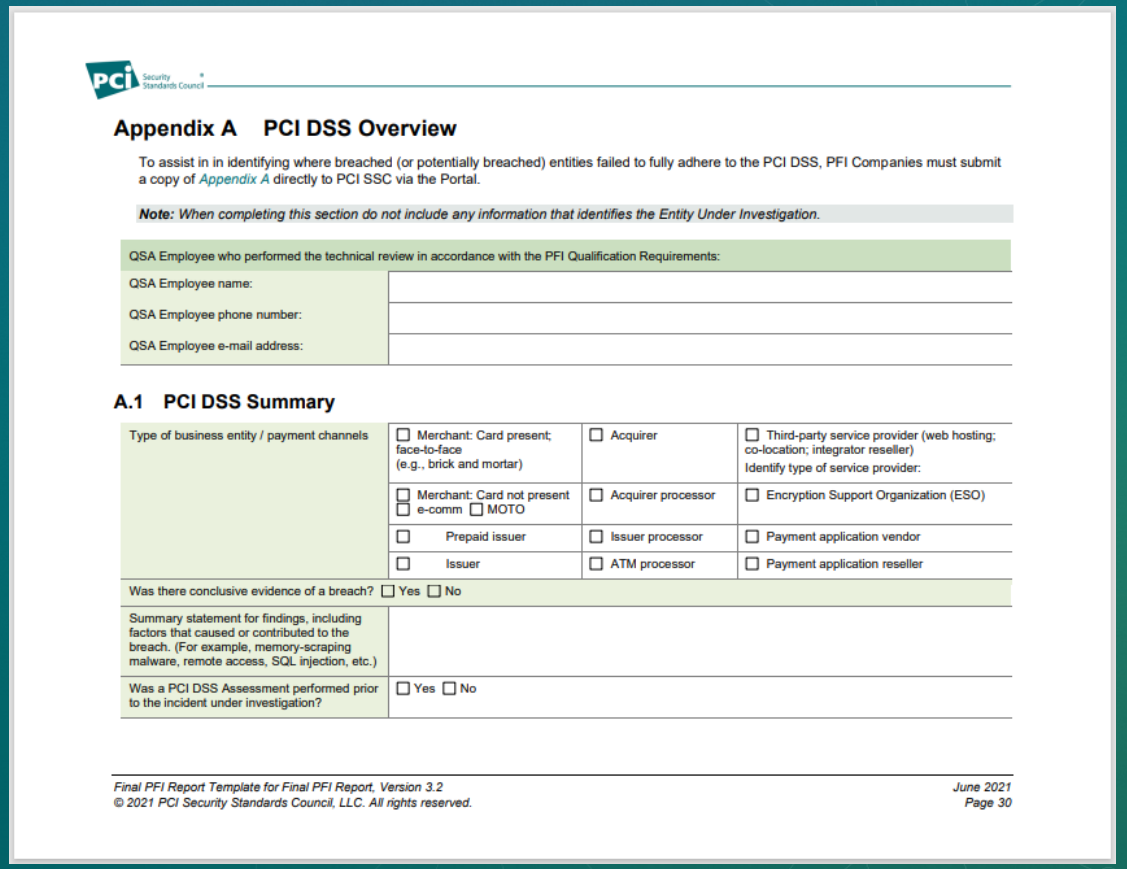


Payment Card Industry (PCI)
Data Security Standard
Final PFI Report

Template for Final PFI Report

Version 3.2

July 2021



Appendix A PCI DSS Overview

To assist in 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	☐ Merchant: Card present; face-to-face (e.g., brick and mortar)	☐ Acquirer	☐ Third-party service provider (web hosting; co-location; integrator reseller) Identify type of service provider:
	☐ Merchant: Card not present ☐ e-comm ☐ MOTO	☐ Acquirer processor	☐ Encryption Support Organization (ESO)
	☐ Prepaid issuer	☐ Issuer processor	☐ Payment application vendor
	☐ Issuer	☐ ATM processor	☐ 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

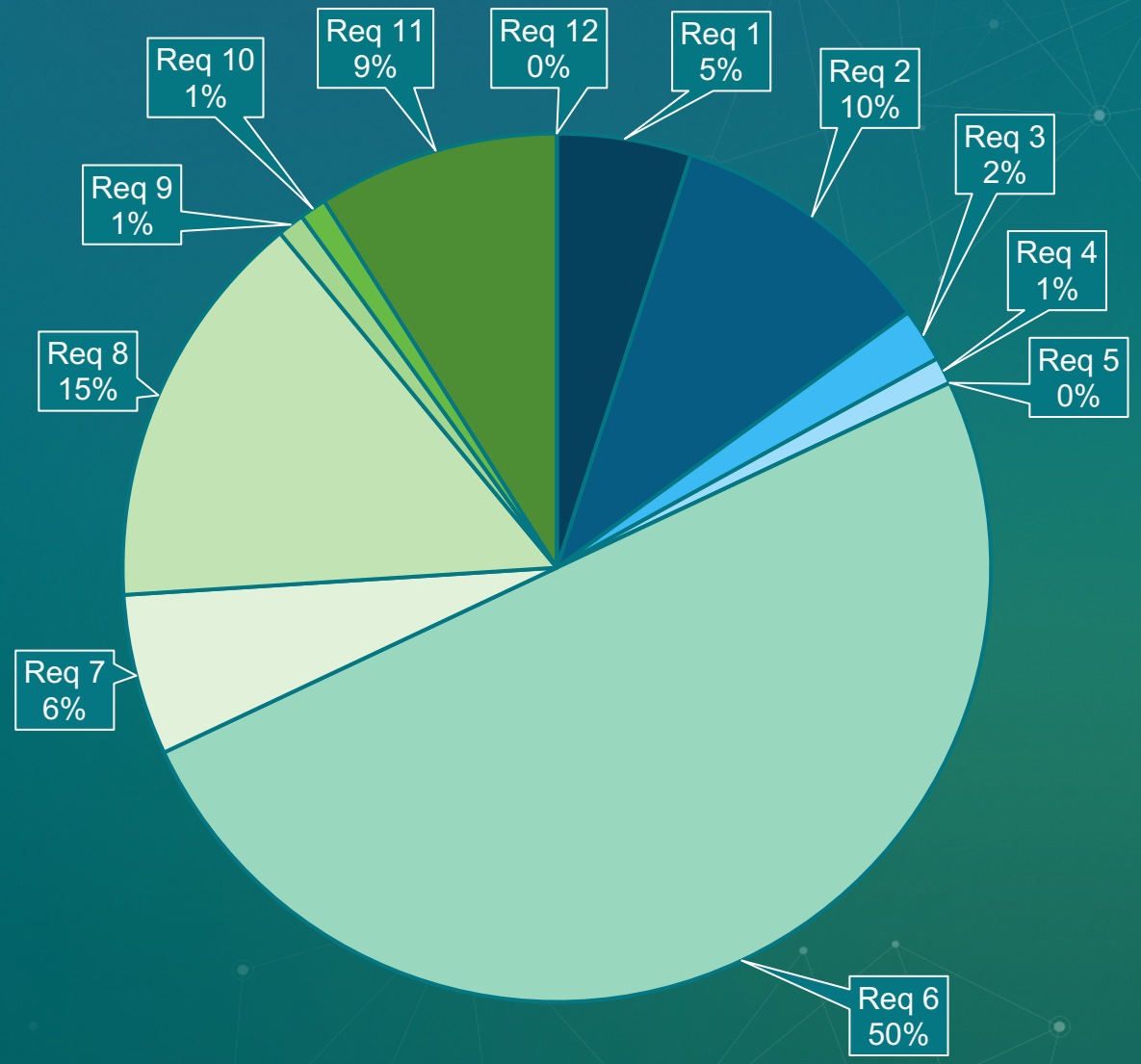
Results remain fairly consistent year-to-year

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

PCI Security Standards Council®

Requirement 8:
Identify and authenticate access to system components

PCI Security Standards Council®

Requirement 11:
Regularly test security systems and processes

PCI Security Standards Council®


Final Insights
from the PFIs
PCi
Security
Standards Council