Lauren Holloway

Director, Data Security Standards

PCI Security Standards Council

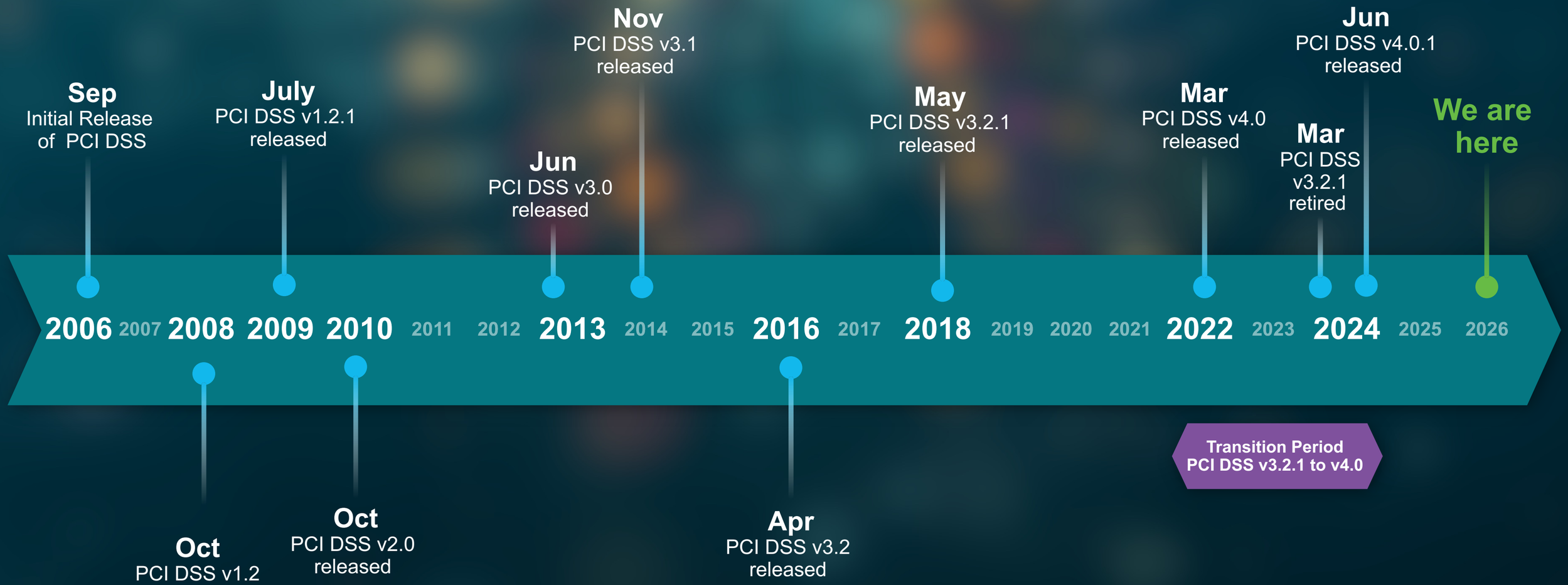




PCI DSS:

The Next Chapter Starts Here

PCI DSS: The Next Chapter Starts Here



The PCI DSS Story

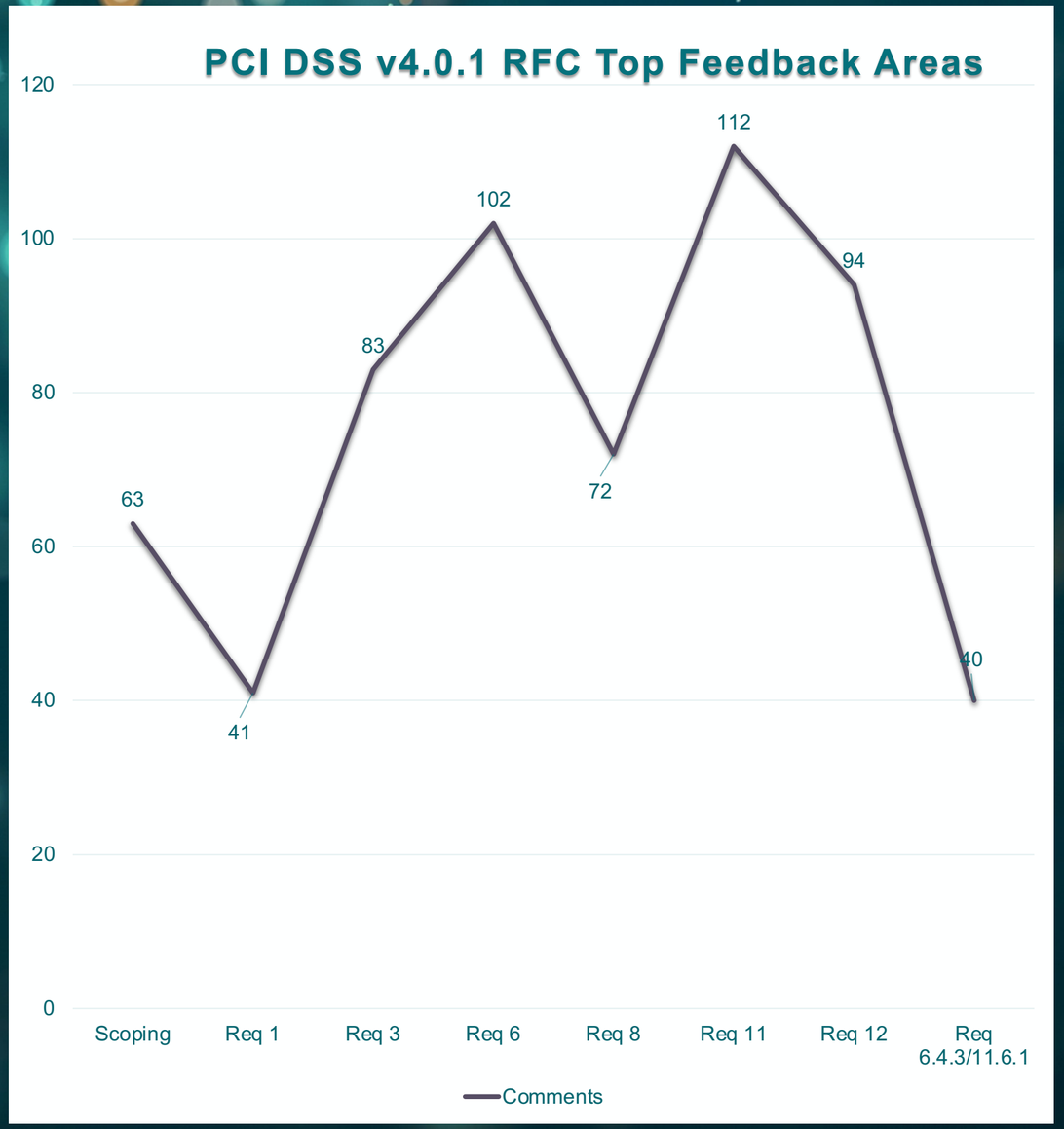
Goals of the PCI DSS Revision

1. Establish environmental security structure not solely based on PAN
2. Provide flexibility to apply security rigor based on risk
3. Define clear scope impact for use of PCI SSC validated solutions
4. Optimize and modernize validation documents

PCI DSS v4.0.1 RFC

From 8 June - 20 July 2026

- 70 companies provided feedback
- 884 comments



Password Complexity

Password Rotation

How MFA Applies

Payment Page Scripts

Scoping

Key Management

AI for Code Development

Passkeys

AI, Cloud, APIs

Prevent Copy and Paste

Keyed Hashing

Vulnerability Management and Patching

Based on RFC Feedback…



Objective-Based Requirements

Clarify Customized Approach and Compensating Controls

Add 3DS Core and TSP into PCI DSS

And AI…



Move 3DS Core and TSP into PCI DSS

PCI DSS will apply to three types of data:

Account Data

- For entities that store, process, transmit account data

3DS Sensitive Data

- Defined in the *PCI 3DS Data Matrix*
- For 3DS Providers that perform or facilitate 3DS transactions

TSP Payment Tokens & Payment Token Data

- For Token Service Providers that generate or issue EMV payment tokens

Appendices will not apply to general PCI DSS population

Objective-Based Requirements

Focus on what to implement, rather than how to implement it

- As needed, to simplify complex or confusing requirements
- Level of detail for most PCI DSS requirements will remain



Combine Customized Approach & Compensating Controls

To address feedback

- One approach for meeting a requirement differently
- Consolidated worksheet to address either option



PCI DSS and AI



Get Involved with Changes to PCI DSS



RFCs for all stakeholders



Frequent meetings with the DE-TGG

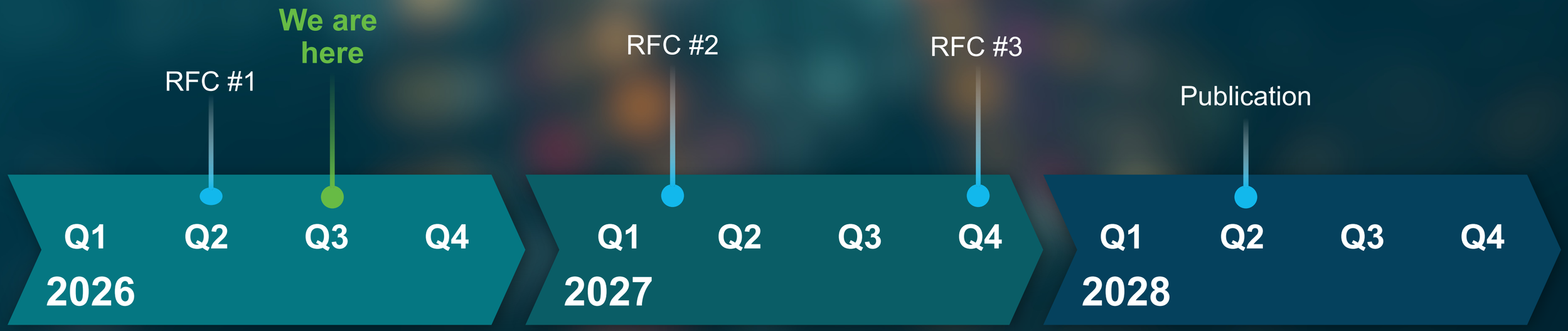


Online collaboration with BoA, GEAR, TGG



Many opportunities to participate – please join us!

Estimated Timeline for Changes to PCI DSS



For illustrative purposes only; dates are subject to change

PCI DSS Recent Guidance

2026 Guidance

- Compensating Controls and the Customized Approach
- PCI DSS to NIST Cybersecurity Framework Mapping
- AI Guidance
- Coming soon: Understanding Third-Party Service Providers

2025 Guidance

- Authentication Guidance
- Vulnerability Management
- Segmentation for Modern Network Architectures
- Integrating AI into PCI Assessments

FAQ Updates

- General updates
- New FAQs

Session Title



Lauren Holloway

Director, Data Security Standards



Andy Barratt

Vice President, Assessments



Jana Ehlers

Director PCI

20 YEARS OF SECURING PAYMENT DATA

Key Takeaways



PCI DSS is evolving to address changes in the payments industry



Changes are based on your feedback



Join us - make sure your voice is heard!