VIKINGCLOUD®

2025 NORTH AMERICA COMMUNITY MEETING

Risk-Directed Security

From enforcers of PCI DSS to enablers of a secure payment ecosystem.

PCI Security Standards Council®

Gabe Moynagh

GM, Acquirer Business Development
VikingCloud

VIKINGCLOUD®

Kevin Pierce

President and Chief Operating Officer
VikingCloud

VIKINGCLOUD®

PCI Security Standards Council®

Today's Discussion.

Agenda

- **A Look Back.**
- **Accelerating Industry Change.**
- **Risk-Directed Security.**
- **Closing Thoughts.**

PCI Security Standards Council

Let’s Get Started.

> **The best way to predict the future is to invent it.**

Alan Kay
Educator and computer pioneer.

> **But to invent wisely, we must first understand what came before.**

Gabe Moynagh
Entrepreneur and PCI pioneer.

PCI Security Standards Council

A Look Back – To Look Forward.

The PCI Security Standards Council was established nearly 20 years ago. A lot has changed.

PCI DSS Timeline

1988-1998
$750 million fraud crisis - Industry facing massive credit card fraud losses

1999-2001
Payment industry response - First brand-specific security standard program launched.

December 2004
PCI DSS 1.0 Launch - Five major card brands create unified standard

September 2006
PCI Security Standards Council established - Global oversight body formed by five founding card brands

October 2010
PCI DSS v2.0 - Major revision for flexibility and clarity

November 2013
PCI DSS v3.0 - Business integration focus (Effective January 2015)

March 2022
PCI DSS v4.0 - Major transformation with customized approach (370→500+ requirements)

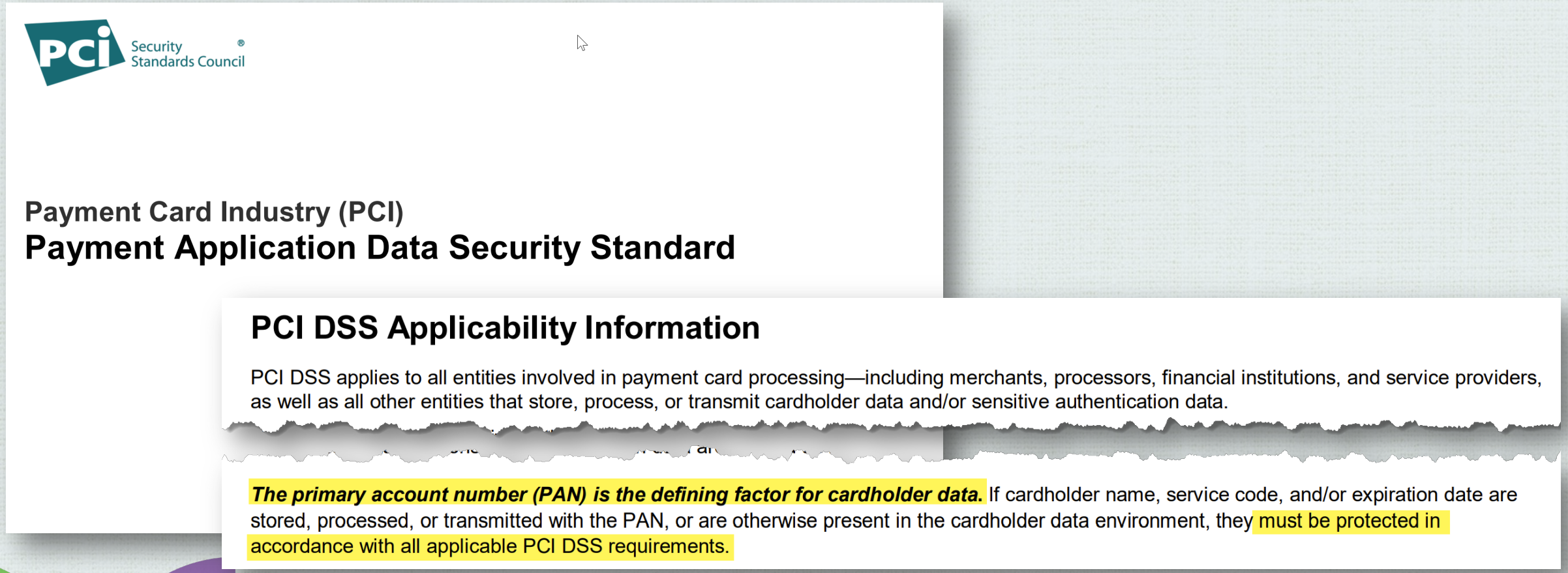
March 2025
CRITICAL DEADLINE - All future-dated v4.0 requirements become mandatory

April 2025:
Payment industry response – First brand-specific risk-directed security-based program announced.

PCI Security Standards Council

A Look Back – to Look Forward.

PCI DSS was designed to protect merchants and service providers—by securing the Primary Account Number—the *"defining factor for cardholder data."*



Payment Card Industry (PCI)

Payment Application Data Security Standard

PCI DSS Applicability Information

PCI DSS applies to all entities involved in payment card processing—including merchants, processors, financial institutions, and service providers, as well as all other entities that store, process, or transmit cardholder data and/or sensitive authentication data.

The primary account number (PAN) is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed, or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all applicable PCI DSS requirements.

A Look Back – to Look Forward.

The PCI DSS has set the baseline—and improved data protection for millions of businesses, service providers, and consumers worldwide.

- **Unified global standard** replacing fragmented card brand requirements.
- **Comprehensive** with successive iterations expanding security controls and data protection procedures to minimize data breach risk.
- **4-tier, tailored compliance system** based on transaction volume.
- **Professional ecosystem** (QSAs, ASVs, SAQs).

Yet ...

Merchant cyber risk is real - and growing.

PCI Security Standards Council

Cyber Risk is Real.

Today, SMBs continue to be the **#1 target for cyber criminals**—mainly because they are unprepared.

74% of SMB owners self-manage cybersecurity or rely on untrained family members or friends; nearly half admit they or their helper lack proper training or full understanding of the risk.

Cybersecurity Incidents Top 3 Consequences

#1 **Business downtime (55%)**

#2 **Loss of customers (36%)**

#3 **Loss of sales (22%)**

Source: VikingCloud SMB Research 2025

Animal Medical Clinic
OF GOOSE CREEK

"All of a sudden, our computers just went down. We got this message saying all our files were encrypted and we needed to pay $10,000 in Bitcoin to get them back. That's a huge amount for a small animal hospital like us… Everything we needed to care for our animals and run our business was gone."

Facility Administrator
Summerville, SC

PCI Security Standards Council

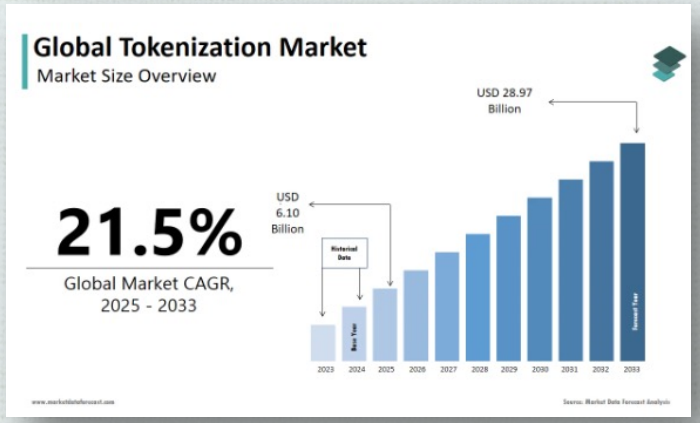
Accelerating Industry Change.

Protecting merchants today means evolving how we secured payment data in the past.

1 PAN is still the key driver for PCI DSS requirements.

PAN (primary account number) is **the defining factor** for cardholder data… must be protected in accordance with all applicable PCI DSS requirements.

2 Industry-wide focus on non-PAN based transactions.



85% of online merchants use tokenization to secure customer payment data.

Global tokenization market growing at a CAGR of 21.5%

3 AI is rapidly changing the threat landscape and attack surface for SMBs.

55% said AI-empowered cybercriminals **are more advanced** than their internal teams.

53% admit AI creating new attack points **for which they are unprepared**.

PCI Security Standards Council

Accelerating Industry Change.

From Baseline to Breakthrough: Building on Compliance to Stay Ahead of Threats

- **Compliance frameworks are essential**—they set a consistent baseline for protecting payment data and uniting the industry around proven controls.
- **But modern threats move faster** than any standard update cycle, which means organizations need adaptive measures on top of that strong compliance foundation.

Compliance-Driven Security:

- Establishes a proven baseline of controls.
- Validates security through regular audits.
- Provides consistency across the payment ecosystem.

PLUS

Risk-Directed Security:

- ✓ Real-time threat prioritization.
- ✓ Adaptive response to evolving tactics.
- ✓ Aligned to merchant unique attack surface.

PCI Security Standards Council

The Question.

Where do we go from here?

Pivoting from compliance enforcement to enabling practical security for all merchants.

RISK-DIRECTED SECURITY

PCI Security Standards Council

What is Risk-Directed Security?

Moves merchant risk remediation from compliance checklists to prioritization based on what matters most:

- **Likelihood of exploitation.**
- **Level of exposure.**
- **Potential business impact.**

Key Elements

1. **Tailored Risk Profiles:** Specific to e-commerce and brick-and-mortar merchants.
2. **Internal + External Assessments:** Beyond what hackers see externally.
3. **Site-specific evaluation:** Customized for each merchant location.
4. **Continuous monitoring:** Monthly assessments, not annual checkups.
5. **Expanded asset protection:** Social media, credentials, beyond traditional IT focus.
6. **Integrated solutions:** Unified platform addressing identified risks.

PCI Security Standards Council

What is Risk-Directed Security?

Dynamic Merchant Cyber Defense

Cyber Risk Assessment and Scoring

- Security Awareness Training
- ID Theft Protection (Dark Web, Online Presence, Credit)
- ID Theft Remediation Support
- Web Malware Scanning
- Endpoint Protection (Anti-virus, Policy Scanning, Threat Detection, IVS)
- Website Script Inventory and Monitoring
- File Integrity Monitoring
- Authenticated Vulnerability Management
- Network Threat Detection
- Web Application Firewall
- BOT Protection
- Security Information & Event Management (SIEM)
- Data Encryption Management

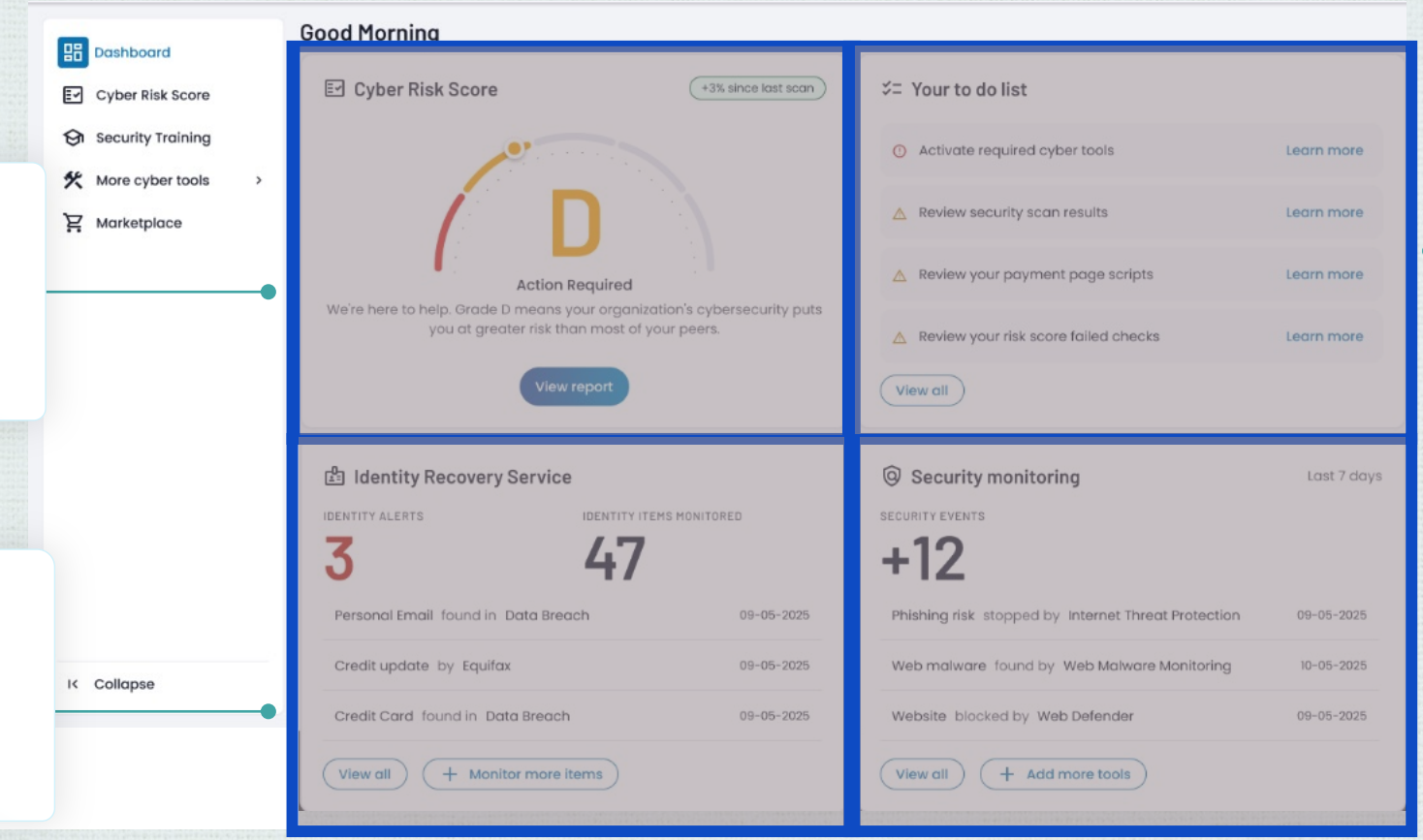
PCI Security Standards Council

Risk-Directed Security In Action

Example: Providing merchant-specific recommendations, actions, and tools to protect their data, their customers, and their business.

External & Internal Risk Assessment

Personal and Social Network Risk



Prioritized Actions Based on Risk Impact

Continuous Monitoring of All Risk Surfaces

PCI Security Standards Council

Why is the Shift Important?

Helping SMBs secure their payment ecosystem.

46%
say their current business has experienced a cyberattack.

Nearly
1 in 5
SMEs who experienced a cyberattack then filed for bankruptcy (18%) or closed the business (17%).

Sources: Payment brand global survey and VikingCloud SMB Research 2025

PCI Security Standards Council

The Risk-Based Transformation

Evolving Security Together

Our Next Steps:

1. **Acknowledge the Gap** – Checking the compliance box vs. active threat defense.
2. **Build the Foundation** – Use compliance as the launchpad for operational cyber defense readiness.
3. **Focus on Context** – Prioritize cyber security actions by business impact and threat intelligence.
4. **Enable Decision-Making** – Equip merchants with the right context through site-specific insight.
5. **Close Security Gaps** – Maintain an ongoing cycle of gap remediation as risks evolve and new vulnerabilities emerge.

VIKINGCLOUD®
BUSINESS UNINTERRUPTED.

> The best way to predict the future is to invent it.

Alan Kay
Educator and computer pioneer.

PCI Security Standards Council

VIKINGCLOUD®
BUSINESS UNINTERRUPTED.

2025 NORTH AMERICA COMMUNITY MEETING

GABE MOYNAGH
GM, Acquirer Business Development

gabemoynagh@vikingcloud.com

KEVIN PIERCE
President and Chief Operating Officer

kevinpierce@vikingcloud.com

PCI Security Standards Council®

PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING