PCI DSS v4.0.1 Data Security Standards: Anomalous Cardholder Data, Scope Drift, and the End of Pause/Resume in PCI Compliance.

Meet the Platypus Problem – Cardholder Data in unusual places, and the architecture that eliminates the anomalous data problem.

Definitions, Detection Requirements and the Human Reality of Compliance.

10th April, 2026 v1.0.1[1] - by Jason Thals, SecurePII Co-Founder, Data Protection Officer and Chief Operating Officer, Bachelor of Science (University of Melbourne), Post Graduate in Radio Communications (Swinbourne Institute of Technology), certified Communications Consultant.

Executive Summary

In my 35 years in Contact Centers across solution architecture, operations management, technology selection and governance, and operational security, I have not come across a standard as relevant to merchant operations as the Data Security Standard issued by the Payment Card Industry Council. When implemented correctly coupled with Merchants[2] adhering to the standards their data assets will be well protected from insider threats, unauthorized accesss and data breach.

PCI DSS v4.0.1 (March 2025 and 2026) is the latest iteration of the standard created when the major card companies (Visa, MasterCard, American Express, Discover, JCB) unified their standards into v1.0 in the early 2000s. It places increased emphasis on continuous monitoring, risk-based control validation, and detection of anomalous behavior affecting cardholder data. Version 4.0.1 of the PCI DSS provides a step change in the standard, and will result in Merchants (and QSAs) relying on manual processes as compensating controls not meeting the standards.

An important concept in the PCI DSS v.4.0.1 Data Security Standards is “Anomalous Cardholder Data.” Anomalous cardholder data encompasses any storage, transmission, access, or retention of cardholder information that deviates from defined scope, documented control intent, or established operational baselines. In plain speak, it’s where a Merchant finds Cardholder Data any place that would not be usual. In Australian, we call it a Platypus Problem as it is our favourite tri-part anomaly: a mammal that lays eggs; with a duck-bill and webbed feet but not an avian; and. produces venom but isn’t a reptile. For example, when Cardholder Data appears in an AI transcript,

[1] Feedback from PCI Audit Professionals, CISOs, Compliance Professionals, is welcomed and can be attributed in future versions if a person provides their written permission for attribution.

[2] A Merchant is any entity accepting Card Not Present payments (on-line or over the phone). All Merchants, worldwide, must adhere to the Payment Card Industry Data Security Standard. Proof of adherence by a third party assessor (QSA) is mandatory for high volume Merchants. Banks and Insurers can demand proof of adherence, and do, when a data breach is reported or evidence of suspicious transaction activity related to the Merchant is detected.

that's a Platypus Problem, i.e., it shouldn't be there but now brings the entire AI system, stored transcript, and handling all within the PCI-DSS 4.0 scope.

A recurring misunderstanding in compliance discussions is the assumption that "anomalous cardholder data" refers solely to Primary Account Numbers (PAN) discovered outside the Cardholder Data Environment (CDE). This interpretation is incomplete and potentially dangerous as looking at a Platypus and thinking it is a harmless duck, right up to the point it hits you with its venom!.

PCI DSS v4.0.1 Data Security Standards require minimum monitoring frequency across:

- Log review
- Automated alerting
- Intrusion detection
- File integrity monitoring
- Data discovery and scope validation
- Risk-based frequency determination

However, compliance effectiveness is not determined solely by adherence to monitoring cadence. It is influenced by how accurately controls reflect real-world human behavior and operational constraints. Compensating controls can create substantial "scope drift". A prime example is Pause-Resume recording. Left unaudited for compliance by most organisations, under the newer PCI-DSS 4.0.1 evidence based standards, Pause-Resume is dead technology. Indeed, Pause-Resume has become a worldwide scourge that has put consumers and businesses at financial and reputational risk.

The cost of compliance under PCI DSS v4.0, combined with the realities of human behavior, explains why many Merchants (any business or government entity taking credit card payments) are choosing to outsource these rigorous controls and checks. This is particularly true of spoken cardholder data, which has the potential to significantly expand a Merchant's CDE into recording systems, AI tools, and communications infrastructure.

This paper provides:

- A technical definition of anomalous cardholder data (without further Platypus references)
- Clarification of its relationship to the CDE
- Detailed examination of PCI DSS v4.0 monitoring requirements
- An expanded view of anomaly detection methodologies
- Analysis of human behavior, and unchecked controls, as a driver of scope drift
- Practical implications for merchants

1. Defining Anomalous Cardholder Data in a PCI Context

The PCI Security Standards Council (PCI SSC) does not limit the definition of "anomalous cardholder data" to data merely found outside the CDE. Instead, anomaly detection within PCI environments relates to deviations from expected system behavior and control design[3]. Rather, anomalous cardholder data may include:

[3] PCI Security Standards Council, PCI DSS v4.0 Overview.

- Cardholder data retained in voice recordings, AI data sets, or collaboration tools
- PAN appearing in non-authorized storage locations
- Cardholder data stored beyond defined retention periods
- Unexpected data replication between systems
- Cardholder data in log files or debugging output
- Unapproved transmission channels
- Unusual access patterns by privileged users

From a control architecture perspective, anomalous cardholder data represents **a breakdown in alignment between policy intent and operational reality**. Thus, a more technically accurate definition is:

> *Anomalous cardholder data refers to cardholder data stored, transmitted, accessed, or retained in ways inconsistent with defined PCI scope, segmentation controls, documented policy, or established security baselines.*

This aligns conceptually with NIST definitions of anomalous system activity as behavior that deviates from expected operational norms[4].

2. The Cardholder Data Environment (CDE) and Scope Integrity

PCI DSS defines the CDE as: "The people, processes, and technologies that store, process, or transmit cardholder data."[5] In practical and simple terms, whatever and wherever a Merchant sees, hears, touches, or processes CHD this defines the CDE.[6]

Scope integrity is central to PCI compliance. Once cardholder data appears outside defined CDE boundaries, segmentation assumptions collapse. However, it is critical to recognize:

- Data inside the CDE can still be anomalous.
- Anomaly does not equal out-of-scope.
- Scope validation requires ongoing verification.

PCI DSS v.4.0.1 Requirement 12.3.2 explicitly mandates periodic data discovery to confirm CDE boundaries[7].

Scope drift often occurs due to:

- Voice-based transaction handling, i.e, "spoken cardholder data"
- System integrations
- Debug logging
- Backup processes

[4] NIST SP 800-61 Rev.2, Computer Security Incident Handling Guide.
[5] PCI DSS v4.0 Glossary, definition of Cardholder Data Environment (CDE).
[6] "*The Hidden Scope: Why Manual Credit Card Entry Over the Phone Brings the Entire Merchant Digital and Physical Evnironment Into PCI-DSS 4.0 Scope – and How New Cloud Technology Solves it.*" Feb 9, 2026. Available at: https://www.securepii.cloud/wp-content/uploads/2026/02/pci-dss-hidden-scope-voice-payments-white-paper.pdf?utm_source=website&utm_medium=whitepaper&utm_campaign=pci_hidden_scope
[7] PCI DSS v4.0 Requirement 12.3.2.

- Workflow exceptions
- Manual intervention during system outages

Without active data discovery, organizations risk operating under outdated scope assumptions.

3. PCI DSS v4.0 Monitoring and Detection Requirements

PCI DSS v4.0 significantly strengthens the requirement for continuous oversight and log analysis.

3.1 Log Review and Security Event Monitoring

Requirement 10.4.1 mandates daily log review across all system components in the CDE[8]. This includes:

- Authentication events
- Administrative actions
- System-level security alerts
- Configuration changes

Requirement 10.4.2 requires automated mechanisms to assist with log review[9]. The purpose is not merely compliance formality but anomaly detection. Similar to many XDR solutions deployed across organizations to raise an alarm on data exfliltration, this concept is extended to the CDE to ensure Merchants are identifying deviations from baseline behavior. Just as NIST SP 800-53 requires continuous monitoring of security-relevant events to detect abnormal patterns[10] and thus the proliferation of XDR solutons, the same applies to the CDE.

3.2 Intrusion Detection and Network Monitoring

Requirement 11.5.1 requires deployment of intrusion detection or intrusion prevention mechanisms[11]. Organizations must:

- Monitor traffic entering and exiting the CDE
- Review alerts promptly
- Investigate suspicious activity

IDS/IPS tools function as anomaly detection systems at the network layer, identifying unexpected traffic flows or data exfiltration attempts.

3.3 File Integrity Monitoring (FIM)

Requirement 11.5.2 requires monitoring of critical files to detect unauthorized changes[12]. FIM serves as a control against anomalous modification of:

- Application binaries

[8] PCI DSS v4.0 Requirement 10.4.1.
[9] PCI DSS v4.0 Requirement 10.4.2.
[10] NIST SP 800-53 Rev.5, Continuous Monitoring Controls.
[11] PCI DSS v4.0 Requirement 11.5.1.
[12] PCI DSS v4.0 Requirement 11.5.2.

- Configuration files
- System libraries

Minimum frequency is weekly, though targeted risk analysis may require more frequent review.

3.4 Data Discovery and Scope Validation

Requirement 12.3.2 mandates periodic data discovery to validate the CDE[13]. This is particularly important for identifying:

- PAN outside expected storage system
- CHD in call recordings
- Data copied to backup archive
- Temporary storage artifacts
- Unstructured data repositories

ISO/IEC 27001 similarly requires asset identification and classification to ensure sensitive data remains controlled within defined boundaries[14].

3.5 Targeted Risk Analysis

Requirement 12.3.1 introduces a risk-based approach to frequency determination[15]. Organizations must:

- Document rationale for monitoring frequency
- Align frequency to threat landscape and operational exposure
- Reassess upon significant changes

This reflects modern governance models emphasizing adaptive risk management over static compliance checklists.

4. Beyond Controls: The Human Behavior Dimension

Security frameworks define controls. Humans execute workflows. The Verizon Data Breach Investigations Report consistently identifies human behavior as a leading contributing factor in security incidents[16]. Stolen identity remains the number one cause of data breach incidents.

Operational realities include:

- System downtime
- Forgotten credentials
- Rushed service interactions
- Device failures
- Customer impatience

[13] PCI DSS v4.0 Requirement 12.3.2.
[14] ISO/IEC 27001:2022, Clause 5 & Annex A asset management controls.
[15] PCI DSS v4.0 Requirement 12.3.1.
[16] Verizon 2023 Data Breach Investigations Report.

When systems restrict legitimate tasks, users seek alternate pathways. Common compensating behaviors:

- Reading PAN aloud during voice calls
- Writing details temporarily on paper
- Sending card information via email
- Storing data locally "just until resolved"

Further to system restrictions, competing organisational requirements, such as Quality Monitoring can significantly impact the effectiveness of a compensating control (approved by the QSA during the annual Report on Compliance with the PCI DSS) like Pause-Resume recording. In many cases I have personally observed in my decades-long career in the contact center industry, the quality team overrides the security team, instructing staff not to pause recording due to misuse of the procedure. A common example of agent misuse relates to an angry customer interaction, where the agent doesn't want to "get caught" responding.

These actions create anomalous cardholder data, often invisible to automated monitoring. ENISA and SANS Institute research emphasize that security controls misaligned with usability increase the likelihood of risky workarounds[17].

Consolidated monitoring frequency overview.

Control	**Requirement**	**Frequency**
Log review	10.4.1	Daily
Automated log review	10.4.2	Daily
IDS/IPS monitoring	11.5.1	Promptly (commonly daily)
File Integrity Monitoring	11.5.2	Weekly minimum
Data discovery (PAN outside CDE)	12.3.2	Quarterly (Annually minimum
Risk assessment	12.3.1	Annually

5. Security Versus Usability: Designing Controls That Hold

Security is most effective when secure behavior is also the easiest behavior. Technology ecosystems that integrate security into natural workflow patterns reduce bypass risk. Where friction is high:

- Users create shadow systems
- Sensitive data accumulates in uncontrolled environments
- Monitoring assumptions fail

Voice channels represent a particularly under-monitored vector, where conversational transactions may expose cardholder data without digital audit trails. For example, if an automatic process fails to pause a recording (e.g. looking for a URL when a payment window opens, but due to network disruptions, the URL is missed by the process) or a manual process is by-passed.

[17] ENISA Threat Landscape Reports; SANS Security Awareness Research.

Aligning compliance architecture with human behavior reduces anomalous exposure at its source rather than detecting it after propagation.

6. A Technology Solution to a Compliance and Data Security Standards Challenge. Practical Guidance for Merchants

Developments in cloud technology coupled with the proliferation of VoIP technology across nearly all Merchants, has enabled a new approach that substantially and materially lowers data protection costs while ensuring CHD entering the CDE is minimal, and minimizing exposure to PCI-DSS 4.0.1 Data Security Standards. Merchants can implement real-time redaction to remove Cardholder Data from calls before exposure to the Merchant CDE. SecurePII's cloud technology for VoIP solutions like Cisco Webex and Genesys is a prime example. This new market entrant removes PAN before it enters the Merchant network. The effect of SecurePII's SecureCall PCI Compliance solution is that the sensitive cardholder data is removed at ingestion whereby it never enters the enterprise network and with tokenization of the credit card, the Merchant does not store any creditcard data. Obviously, not having the PAN in the network substantially reduces the cost of monitoring and securing data. Outsourcing PCI DSS compliance to SecurePII for the Voice channel entitles the merchant to reduce the scope of its CDE and thereby satisfy large sections of its annual report on compliance with the PCI DSS.

Without such a utility, each Merchant must undertake a series of regular checks and reporting to maintain a robust compliance posture for all channels including Voice:

- Conduct daily log review per Requirement 10.4.1
- Implement automated alerting mechanisms
- Review IDS/IPS alerts promptly
- Monitor file integrity regularly
- Conduct annual minimum data discovery scans
- Perform documented targeted risk analysis
- Evaluate operational workflows for potential workaround risks
- Ensure all transaction channels — including voice — are assessed for exposure

Compliance is not static; it is a continuous validation of scope, behavior, and system integrity.

7. Conclusion

PCI DSS v4.0.1 provides an essential guardrail to businesses and government processing credit cards. It must be implemented faithfully and operated with diligence and rigor. Where cardholder details are exposed to a Merchant, adherence to the standard is expensive and vulnerable to people, technology and process failure.

Effective compliance integrates governance, monitoring, usability, and behavioral awareness. Security systems designed without regard to operational reality frequently generate the anomalies they aim to prevent. Continuous, daily monitoring for "anomalous data" and quarterly and annual evidence gathering are essential to stay true to the standard. These are expensive.

Employing a service like SecurePII's SecureCall PCI Compliance, to remove cardholder details at ingestion and outside the Merchant boundary, exponentially reduces the PCI compliance cost and significantly improves adherence to PCI Data Security Standards. It allows business and government to protect customer data and themselves from the reputational damage of (avoidable) data breaches.

✍️ Jason Thals, COO, SecurePII
🔗 https://www.linkedin.com/company/securepii/
🤝 https://www.securepii.cloud/contact/
🌐 https://www.securepii.cloud/