The Hidden Scope: Why Manual Credit Card Entry Over the Phone Brings the Entire Merchant Digital and Physical Environment Into PCI-DSS 4.0 Scope — And How New Cloud Technology Solves It.

February 9, 2026 v.1.0.[1] *By, William Placke, Certified Information Privacy Professional-US (CIPP-US), Juris Doctorate, Diploma EU Law, HBS Certificate in Data Privacy and Data Security, President SecurePII Americas.*

*This publication is informational and not legal or professional advice. Please consult your legal counsel, auditor, QSA and/or ISA for advice specific to your facts and circumstance*s.

Executive Summary

This whitepaper provides a comprehensive and authoritative analysis of why manual card entry based on spoken card data over the telephone creates full and increased PCI-DSS 4.0 scope for merchants of all sizes. In our experience, there is a mistaken view of the scope of PCI-DSS when spoken credit cards are taken by enterprise, whether from a single location up to large call centers. PCI-DSS v4.0 replaced v 3.2.1 after March 31, 2024, with certain new requirements becoming mandatory on March 31, 2025. New requirements requiring not just self-attestation but additional evidence, will have Qualified Security Assessors and Internal Security Assessors increasing focus on both the digital and physical environments.

The straight-forward visual is that when credit card information is spoken over the phone, the scope of PCI compliance includes everywhere that credit card information can be heard, seen, or digitally touched, including the physical location such as desk environment.[2] Each one of these areas must be examined for PCI compliance. This is particularly challenging where call center agents or payments are made with work-from-

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

[2] *See*, Payment Card Industry Data Security Standard: *Requirements and Testing Procedures, v4.0.1* (June 2024) Requirement 9: Physical Access to Cardholder Data at page 210: "Any physical access to cardholder data or systems that store, process, or transmit cardholder data provides the opportunity for individuals to access and/or remove systems or hardcopies containing cardholder data; therefore, physical access should be appropriately restricted."

home agents. The spoken credit card has been variously referred to as "keyed entry", "manual card entry" and "Card-Not-Present" or MOTO transactions.

Quite simply, if the enterprise accepts spoken credit card data over the phone, PCI DSS scope expands materially because people, process, digital environment, physical environment, and technology used to receive that data are in scope. The PCI Security Standards Council guidance is explicit: "***Accepting spoken account data over the telephone puts personnel, the technology used, and the infrastructure to which that technology is connected into scope of PCI DSS***."[3]

This paper addresses widespread misconceptions about scope of PCI compliance, provides detailed analysis of Cardholder Data ("**CHD"**) flow and the Cardholder Data Environment ("**CDE**"), shows where prior industry practise of taking credit cards over the phone and inputting into a device may violate PCI-DSS 4.0 standards without the mitigation of temporary compensating controls, and outlines modern solutions that align with PCI scoping rules as significantly and substantively expanded with new PCI-DSS 4.0 standards.

The document is structured to stand on its own as an industry resource, providing PCI standards knowledge relating to voice transmission of credit card data before introducing any solution. This document is an appropriate resource for PCI Auditors, Qualified Security Assessors, Internal Security Assessors, CISOs, Compliance Professionals, Information Security Professionals, Finance Directors, and Cybersecurity Professionals.

Introduction: Telephone Payments – The Last Unsecured Channel

Across industries, merchants continue to rely on telephone payments. Retail stores accept phone orders, utilities take payments by phone, government agencies collect fees, and healthcare providers process billing. According to the Federal Reserve Bank of Kansas City in research published in May 2025, in the United States, the amount of commerce conducted in "Card-Not-Present" transactions, single-message networks for non-prepaid debit, have increased over 300% from $26B in 2011 to $85B in 2021, the most recent available data set.[4]

---

[3] PCI Security Standards Council, Information Supplement: *Protecting Telephone-Based Payment Card Data,* at p. 4. Available at: https://listings.pcisecuritystandards.org/documents/Protecting_Telephone_Based_Payment_Card_Data_v3-0_nov_2018.pdf

[4] *See*, Federal Reserve Bank of Kansas City, Fumiko Hayashi, "*Card Not Present Fraud Rates in the United States after the Migration to Chip Cards*." May 21, 2025. Available at: https://www.kansascityfed.org/research/payments-system-research-briefings/card-not-present-fraud-rates-in-the-united-states-after-the-migration-to-chip-cards/

With the introduction of Chip technology in credit cards, the amount of Card Present fraud went down globally.[5] Chip technology "was intended to mitigate card-present fraud from counterfeit cards, and in many countries, committing card-present fraud indeed became much more difficult after [chip] migration. As a result, fraudsters shifted their targets to card-not-present transactions."[6] It is a surprising, if not obvious, realization that Chip and PIN technology innovation to reduce in-person credit card fraud, would lead to bad actors doubling down in Card-Not-Present transactions. In fact, a November 2025 FICO Blog post "Card-Not-Present fraud is projected to reach an unbelievable $49 billion globally, and looks set to remain a leading channel for criminals."[7]

Despite the "unbelievable" amount of fraud in the CNP channel, within the CNP channel, the voice channel remains one of the least understood areas of PCI-DSS; and, in reality, the channel that seems to have been the last to innovate, until recently. That is, many enterprises still ask a customer for their credit card information over the phone and then type that credit card information into a credit card terminal. Some add in requiring the agent to pause/resume call recordings to make sure the digital systems do not capture credit card data. It is urged, that relatively speaking to all other advances in cybersecurity around payments, this method of commerce should be relegated to mild amusement in "in the past we used to take credit cards over the phone, type them into a webpage or terminal, and rely on humans to pause and resume . . . ." with a good chuckle at how primitive the voice channel security remained for so long.

The practical reality is that every time a "pause" request fails or an agent forgets to pause a recording, another potential exposure is added to the merchant's cache of validated credit cards[8]. Given typical contact centre workloads, even a small proportion of payment calls can result in agents handling hundreds of card transactions annually, meaning that low failure rates in manual controls can accumulate significant exposure over time. Even a small failure rate in pause recording controls can accumulate significant exposure over time. For example, if agents handle hundreds of payment interactions annually, a hypothetical 1% failure rate could result in multiple card details being unintentionally captured each year. Over typical recording retention periods of five to seven years, this could translate into thousands of exposed card numbers within a modest sized contact center.Many organizations, including large enterprises, believe incorrectly that PCI requirements are satisfied because they use PCI-approved terminals, web interfaces, PCI-certified carriers, or cloud platforms with their own PCI certifications. This paper reduces the confusion and explains why PCI scope starts where CHD (Cardholder Data) first

---

[5] *Id.* "The card-not-present fraud rate significantly increased in many countries during the 2010s immediately after migration to EMV chip-card technology." Citing Sullivan 2013; and Markiwicz and Sullivan 2017.

[6] *Id.*

[7] *See*, FICO Blog, by Debbie Cobb, "*Card-Not-Present Fraud Remains a Leading Concern as Payment Systems Evolve.*" November 12, 2025

[8] PCI Security Standards Council. *Protecting Telephone-Based Payment Card Data*, Information Supplement, Version 3.0, November 2018, page 37. Available at: https://www.pcisecuritystandards.org/documents/Protecting_Telephone_Based_Payment_Card_Data_v3-0_nov_2018.pdf

appears which is often in the merchant environment before it reaches any secure terminal. At the heart of the analysis is that the audit scope is determined by where the CHD and Sensitive Authentication Data ("**SAD**") are stored, processed or transmitted in addition to connected system components including any AI tools operating on that CHD/SAD. The Cardholder Data Environment similarly extends both digitally and physically.[9]

PCI-DSS 4.0 Scoping Principles

When large parts of PCI-DSS 4.0 became effective in March 2025 updating from v3.2.1 effective June 2018, it reinforced the principle that PCI scope follows the data. Scope includes personnel and the technology and infrastructure involved in receiving spoken account data, plus the physical areas (e.g., retail counter, desk, cubicle, home office) where CHD could be observed, recorded, written down, or otherwise captured during the payment process. That is, any digital or physical environment where primary account number ("PAN"), cardholder data ("CHD") or sensitive authentication data ("SAD") can be heard, seen, processed, transmitted or stored is in PCI scope.[10]

Key scoping principles include:

1. CHD first appearance determines scope and comprises the Cardholder Data Environment.
2. Voice channels are considered in-scope transmission channels.
3. Human agents who hear CHD are in-scope and if anyone within hearing can hear that CHD that entire environment is in scope (think, agent repeating numbers out loud or on a speaker phone when typing in the CHD).
4. Any system capable of capturing CHD is in scope, including:
    a. Call recordings
    b. Voice analytics including sentiment analysis engines
    c. AI/LLM transcription engines
    d. Desktop applications
    e. Screen capture tools
    f. Log aggregation platforms
    g. Monitoring tools
5. PCI Point-to-Point Encrypted terminals can reduce scope if CHD enters the terminal first and without simultaneous voice transmission of the data but not if the agent hears CHD and then keys it.[11]

---

[9] *See*, Payment Card Industry Data Security Standard: *Requirements and Testing Procedures, v4.0.1* (June 2024) Requirement 9: Physical Access to Cardholder Data at page 210.

[10] *See,* Payment Card Industry Data Security Standard, Self-Assessment Questionnaire A and Attestation of Compliance for use with PCI DSS Version 4.0. Available at: https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4-0-SAQ-A.pdf

[11] For example, Clover, a provider of Point-to-Point encrypted terminals has a MOTO enabled virtual terminal. Yet, at the same time, explicitly states the qualification that "Businesses must follow Payment Card Industry Data Security Standards (PCI-DSS) to protect customer data." Reinforcing that while the terminal itself may be PCI compliant, the requirements of the environment, physical and digital, where the

6. The merchant digital and physical environment must stand on its own at the moment that environment has access to CHD

These principles form the foundation for understanding why manual card entry by a merchant or call center agent dramatically expands scope.

Under PCI-DSS 4.0, the breadth of the scope is as broad as possible in being applicable to any entity taking credit card information. Any merchant environment where an employee hears, sees, or processes card data by phone is in PCI scope, including Retail stores, Government offices, Utilities, Telecommunications providers, Healthcare practices, Hospitality reservations, Insurance brokers, Real estate/title companies, Financial services, Nonprofits and universities. The number of locations does not affect the applicability of PCI-DSS. A single clerk taking a single payment over the phone triggers the same scope obligations as a large contact center.[12]

Anatomy of a Voice-Based Manual Entry Transaction

A walkthrough of a typical CHD flow during a phone payment reveals the scope problem clearly:

Step 1: Customer calls merchant (or merchant calls customer).

Step 2: Merchant telephony provider routes the call.

Step 3: Merchant UC/voice system receives audio stream.

Step 4: Agent hears the full card number, expiration, and CVV.

Step 5: Voice is rendered by softphone or desk phone.

Step 6: Desktop systems process the session.

Step 7: Call recordings may capture the CHD.

Step 8: Analytics or AI tools may transcribe the CHD.

---

cardholder data (the, "Cardholder Data Environment, or "CDE") is seen, heard, processed, stored, etc. is all in scope for PCI-DSS 4.0. *See*, https://uk.clover.com/insights/card-payments-over-the-phone-how-do-they-work/

[12] *Id* at 2.3 "Telephone environments can vary enormously in size and complexity from a small merchant in a simple telephone environment or reception desk where payments are taken over a single telephone line, to a large, complex, multi-site environment or call center operation able to process hundreds of card payment transactions simultaneously."

Step 9: Agent types the CHD into a terminal. If the agent's system is running slow, they may write the card details down, or type into Notepad or similar, so they can be entered later.

Step 10: Terminal encrypts the card data.

Because steps one through nine occur without redacting or removing the CHD, the merchant is the first point of CHD ingestion and is the focus of the PCI Scope. That the terminal, carrier, or CCaaS provider may have PCI compliant technologies, is not a replacement for the merchant or call center environment itself. They are stand alone assessments. The below diagram 4 from the PCI Security Standards Council makes clear that Steps 1 – 9 are all within scope.[13]

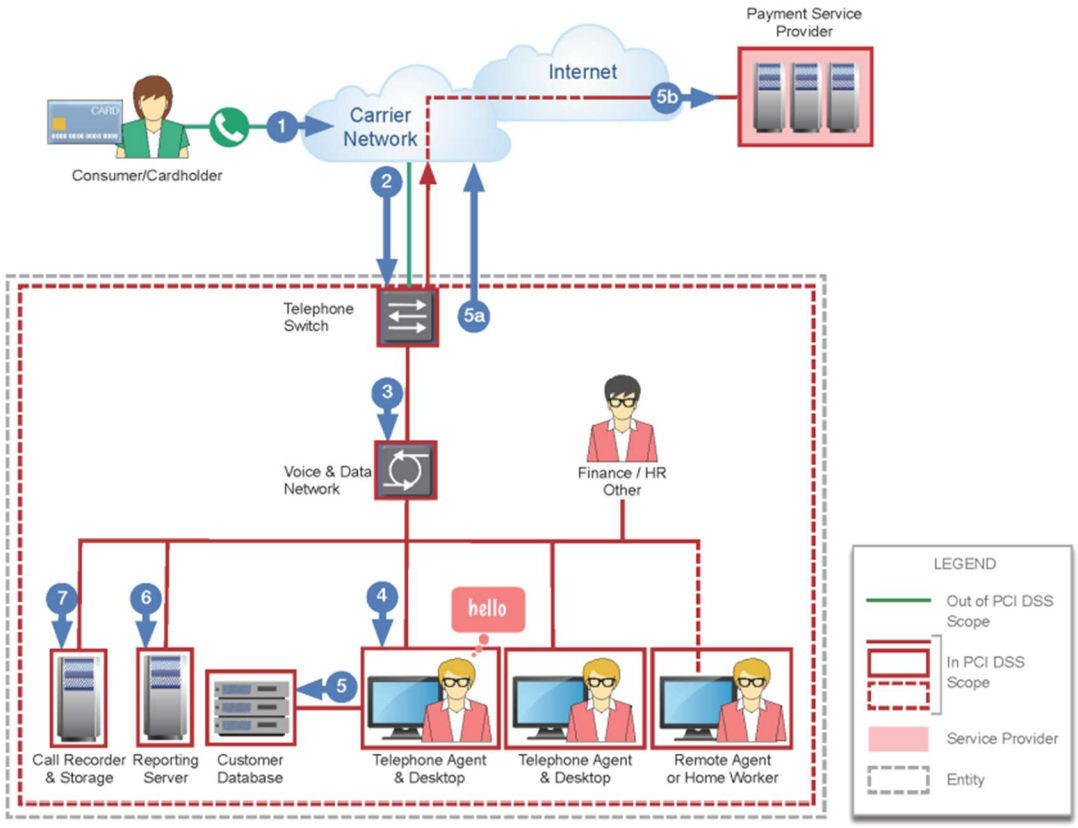


Diagram 4: Telephone environment and call flow where CHD is captured and stored

Merchant Misconceptions Observed in the Market

With quite surprising frequency, we have observed a number of misconceptions repeatedly across RFPs, audits, and vendor claims including:

[13] *Source*: PCI Security Standards Council, Protecting Telephone Based Payment Card Data v3.0. at https://listings.pcisecuritystandards.org/documents/Protecting_Telephone_Based_Payment_Card_Data_v3-0_nov_2018.pdf

1. "*If my carrier is PCI-certified, then I am PCI-compliant*."

Incorrect. Carrier compliance applies only to their systems and stops once it enters the enterprise or merchant network which itself will be examined on its own.[14]

2. "*Our data center is PCI-certified, so phone-based payments are compliant*."

Incorrect. Data center certification does not extend to phone interactions or agent desktops. The merchant or call center environment will be assessed on its own.[15]

3. "*Our terminal is PCI-approved; therefore we are compliant*."

Incorrect. Scope includes personnel and the technology/infrastructure involved in receiving spoken data and including the physical areas and controls where CHD could be observed, recorded, written down or otherwise captured during the payment process.[16]

4. "*We only have one location; PCI scope doesn't apply the same way*."

Incorrect. PCI scope applies regardless of merchant size.[17]

5. "*Our auditor signs off, so we must be compliant*."

Not necessarily. Auditors output is only as good as the input. Some sign-offs rely on outdated interpretations pre-PCI-DSS 4.0, incomplete documentation, or incomplete information. Strengthening requirements under v.4.0 include examining electronic screen shots, config files, audit logs and physical data files. Further evidence requires observing personnel performing a task or process, environmental conditions and physical controls. Last is interviewing the individual personnel getting descriptions of how credit card information is taken over the phone, where the personnel are physically located, the physical environment and the controls over each.[18] An auditor may describe why the requirement standard cannot be met due to business

---

[14] *Id. , at pp 14-15* "If at any point an entity stores, processes, or transmits account data within its environment, the entity's systems and networks through which the account data is stored, processed or transmitted fall within the scope of the PCI DSS, and applicable PCI DSS Requirements must be met irrespective of the type of network the entity has deployed."

[15] *Id at p 15 "*Any entity, system component, network, and third-party service provider with access to CDE must be identified and that access must be secured with applicable PCI-DSS controls."

[16] *Id at p 17:* "All personnel having access to payment card data are in scope of PCI-DSS and should be trained per Requirements 12.6.1 and 12.6.2 and screened as detailed in Requirement 12.7 . . . . A policy should be put in place to ensure that payment card data is protected against unauthorized viewing, copying, or scanning, in particular on desks." *See further* the Clover example in footnote 8.

[17] *Id:* "The telephone environment, whether large or small, provides significant opportunities for payment card data to be compromised outside the organization . . . ."

[18] *See page iv:* Payment Card Industry Data Security Standard Self Assessment Questionnaire A and Attestation of Compliance – for use with PCI DSS Version 4.0. available at https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4-0-SAQ-A.pdf *See further*, section 3.2 "Storage of Account Data is kept to a minimum" at page 4.

constraints and document the Compensating Controls.[19] However, Compensating Controls are only to be used as temporary measures as a bridge to compliance with the control standard.

Correcting these misunderstandings is essential for proper PCI-DSS 4.0 compliance.

Correction of the Most Persistent PCI Myth: Component Compliance Does Not Equal Merchant Compliance

One of the most dangerous and persistent myths is that compliance of a single component (terminal, carrier, CCaaS platform, or data center) provides end-to-end coverage for the merchant. PCI-DSS v. 4.0 explicitly rejects the so called "inherited compliance." The Scope applies to the merchant environment wherever CHD is heard, seen, or processed.

Impact of Manual Card Entry on PCI Scope

The consequences of keyed entry and manual entry span Operations, Security, Technology and Regulatory. The depth of security assessment is typically classified as from Tier 1 to Tier 4 but may vary as each credit card operator can set their own classification such that Visa may differ from Mastercard. Generally, the categories are based on the number of transactions completed in a year as follows: Level 1 (highest level) completing over six million transactions per annum; Level 2: 1 to 6 million transactions annually; Level 3: 20,000 to 1 million transactions annually; and, Level 4: Fewer than 20,000 transactions annually.[20]

Noting that every transaction, across any channel counts and PCI DSS is assessed across all channels and merchant touch-points. The voice channel must meet the same rigorous compliance criteria as online, irrespective of the relative volume processed per channel.

Many companies will find themselves put into the Level 1 Penalty Box for a period in the event of a credit card breach regardless of number or amount of transactions.[21] Additional focus on compliance can also be applied by a merchant's bank if patterns of fraud (including excessive charge-backs) are observed by the merchant's bank.

---

[19] *Id at Appendix B page 22.* Enterprise should be particularly attentive to the Compensating Controls listed. Please note that a Compensating Control is a deviation from the standard required due to business constraints. In the event of a breach, a documented compensating control could lead liablity, an SEC required disclosure in Risk Factors and/or after breach disclosure.

[20] JP Morgan, "What is PCI Compliance" May 25, 2025 available at https://www.jpmorgan.com/insights/payments/security-trust/pci-compliance-guide-protect-payment-data-and-prevent-fraud

[21] Additionally, credit card companies can issue fines for non-compliance. *See* Visa, "*Account Ifnroamtion Security Program and PCI, Protect Cardholder Data*" available at https://corporate.visa.com/en/resources/security-compliance.html "If a service provider or merchant does not comply with the PCI-DSS compliance or fails to rectify a security issue, Visa may assess a non-compliance assessment to the issuer or acquirer."

In our experience and supported by industry reports, third-party assessment costs for a Report on Compliance ("**ROC**") can range from tens of thousands of dollars up to several hundred thousand dollars depending on environment complexity, number of locations, and depth and breadth of in-scope systems.[22]

While the extent of the impact on keyed entry and manual entry of CHD could take an entire book, a short summary of the impacts are as follows:

- *Operational Impact*: Expanded annual PCI assessment scope; Increased employee and contractor training requirements for how to handle CHD and prohibitions on the physical environment; and, more evidence gathering, documentation, and audits.
- *The Cybersecurity and Physical Security Impacts include*: Exposure of CHD to voice recordings and corruption of data where an employee or agent misses the Pause/Resume causing the entire data set to be corrupted; CHD appearing in AI transcripts especially AI notetakers or malicious actors recording on other devices such as a mobile phone nearby.; and CHD captured in logs, analytics, or monitoring tools; and, the most prevalent cybersecurity threat follows through to PCI where insider threats and malicious actors obtain CHD.
- *The Technology Impact includes*: Restrictions on cloud analytics and AI tools given the nature of credit card data as a form of Personally Identifiable Information together with the myriad of rules and regulations around data privacy that go well beyond PCI Compliance (e.g., GDPR, HIPAA, CCPA); Legacy systems forced into scope; More complex penetration testing and assessment of third-party service providers.

QSA and ISA Testing Focus on PAN, SAD, and CHD Taken Over the Phone.

Whether through a self-assessment questionnaire or third-party Qualified Security Assessor conducting the PCI Audit, legacy processes are expensive, time consuming, and leave multiple vectors of attack for bad actors to obtain CHD. Auditors will focus on how secure processes, software, infrastructure, and environments are and whether they meet the standard. Below is an example of the requirements when using a legacy system of taking credit cards over the phone and punching them into a soft client or point-to-point terminal device. This will then be contrasted to new technology available in the market that substantially and materially reduces scope, and therefore cost, of PCI Compliance.

Current State 1: Merchant employee or agent takes Primary Account Number ("PAN") and CHD over the phone, inputs the card data into a point-to-point terminal or web client (such as Verifone or Stripe), and uses pause/resume call recording.

[22] SecurityMetrics: *How Much Does PCI Compliance Cost* by Gary Glover. Available at: https://www.securitymetrics.com/blog/how-much-does-pci-compliance-cost

What the QSA will treat as In-Scope for PCI-DSS 4.0:

1. *People and Procedures*: agents, supervisors, QA, workforce management, anyone who can access recordings, anyone who can see, read or hear the CHD, and anyone who can impact how CHD is handled, and additionally including the annual training required of each on how to handle Card Holder Data.[23]
2. *Technology Path*: softphones, endpoints, handsets, VDI, recording, AI sentiment analysis engines, transcriptions including AI summary and call recordings, QA Analytics, telephony infrastructure, supporting networks, Identity and Access Management including twelve character password rotated every 90 days and/or MFA.[24]
3. Evidence increases because the QSA must validate that the CHD and SAD are not recorded whether by the presence of company sanctioned equipment or an agent personal device such as a smart phone with call recording capabilities becoming more ubiquitous with AI applications. Importantly in Pause/Resume environments, whether a system relies on perfect human execution is to be examined.

In completing a Report on Compliance (ROC), the testing and evidence exhausts close to 400 pages of material in the PCI DSS Requirements and Testing Procedures v. 4.0.1. Summarizing 400 pages is not possible with any justice. But, at the highest level, and in particular to voice environments using pause/resume or transfers to an automated payment platform, a QSA or ISA, will focus on:

1. Proving the CDE boundary with call flows, data flow diagrams, and what technologies, systems or processes may impact the security of the CHD and PAN.
2. Sample and test call process, call recordings, screen recordings, QA tools, and any transcription or indexing capability. Recordings are searchable and can be copied and therefore are frequently the source of control failures. The PCI Security Standards Council has emphasized that because call recordings can be queried, SAD can never be stored even if encrypted.
3. Enforcement of privilege access management ("**PAM**) principles.[25] Validate training on handling of CHD and cybersecurity basics such as the normal phishing trainings ensuring that these trainings are both current and given on at least an annual basis and after initial hiring.[26] A sampling of interviewing employees or agents is routinely done as a matter of course as set forth in Requirement 8.3.8 of the Payment Card Industry Data Security Standard: Requirements and Testing

[23] Payment Card Industry Data Security Standard, Requirements and Testing Procedures Version 4.0.1 June 2024 Requirement 12.6.3.1 at page 312.
[24] Payment Card Industry Data Security Standard, Requirements and Testing Procedures Version 4.0.1 June 2024 at pages 188-191 requirements 8.3.
[25] Payment Card Industry Data Security Standard, Requirements and Testing Procedures Version 4.0.1 June 2024 at page 169 requirement 7.2.5.
[26] Payment Card Industry Data Security Standard, Requirements and Testing Procedures Version 4.0.1 June 2024. PCI DSS Sampling Considerations and requirement 8.3.8 at page 192 and requirement 12.6 at pages 309-313.

Procedures v. 4.0.1 (June 2024) at page 192: "Interview users to verify that they are familiar with authentications policies and procedures."

4. Validating screening and background checks on personnel with access to CHD and the environment.[27]
5. Validating third party service provider management for recording platforms, UCaaS, CCaaS, transcription, analytics, and any managed services (including responsibility matrix).
6. With the ubiquitous availability of AI technologies that leverage sentiment analysis or summarize calls in an AI transcription, it is easy to opine that these technologies now fall well within the scope of PCI-DSS 4.0.[28]

All of this leads not just to the heavy expense of both internal and external assessors, but much time from internal teams required to document, upload evidence, and support the PCI Audit. It is easy to see how and when the annual testing costs upwards of $200,000 with internal and external costs, not to mention the distraction the internal tech teams need to have to provide all the evidence required.

SecurePII's *SecureCall PCI Compliance* product is an effective alternative that enables an architectural solution to the audited scope of the enterprise network when processing CHD, SAD, and PAN, drastically limiting the CDE. The effect of which permits an enterprise to essentially "outsource" its voice PCI Compliance reducing this cost to a minimum. SecureCall is designed to eliminate spoken CHD, PAN, and SAD in the enterprise environment by inserting a PCI DSS validated SecureCall environment into the call only for the payment segment and having the actual CHD and SAD input via DTMF by the cardholder. For example, at the appropriate time in the call for taking payment by phone, the agent/merchant would say to the cardholder, "We at Company X do not hear, see, or store your credit card information. When I prompt you, and without telling me any of the numbers, can you please input your credit card number using the dial pad on the phone you called in on." The cardholder keys in the credit card number, CVC, expiration date, and even zip/postal code while the agent only sees **** and a green checkmark for a valid card. SecureCall integrates with the enterprise chosen payment gateway to send the CHD and SAD directly to the payment gateway without the information ever touching the enterprise network but receiving the payment and/or tokenization confirmation from the payment gateway. The practical PCI audit assessment consequence is that the enterprise

[27] *See*, Payment Card Industry Data Security Standard, Requirements and Testing Procedures Version 4.0.1 June 2024 Requirement 12.7 at page 314. "Performing thorough sreening prior to hiring potential personnel who are expected to be given access to CDE (Cardholder Data Environment) provides entities with the information necessary to make informed risk decisions regarding personnel they hire that will have access to the CDE."

[28] While neither new AI summary and transcription technologies nor sentiment analysis engines are specifically mentioned in the new PCI-DSS 4.0 standards, it would be very well expected, if not obvious, that these would be included within PCI-DSS 4.0 to the extent that cardholder data is ever present at any time, even if later redacted. There is a particular danger that credit card data finds its way into Large Language Models (LLMs). This would then indicate that the entire LLM becomes subject to PCI DSS 4.0, in addition to every privacy law that could be impacted from CCPA to GDPR and beyond.

is no longer accepting spoken account data, which is the trigger for pulling personnel, desktops, networks, and recordings into scope.

With SecureCall in place what a QSA or ISA typically focuses on instead:

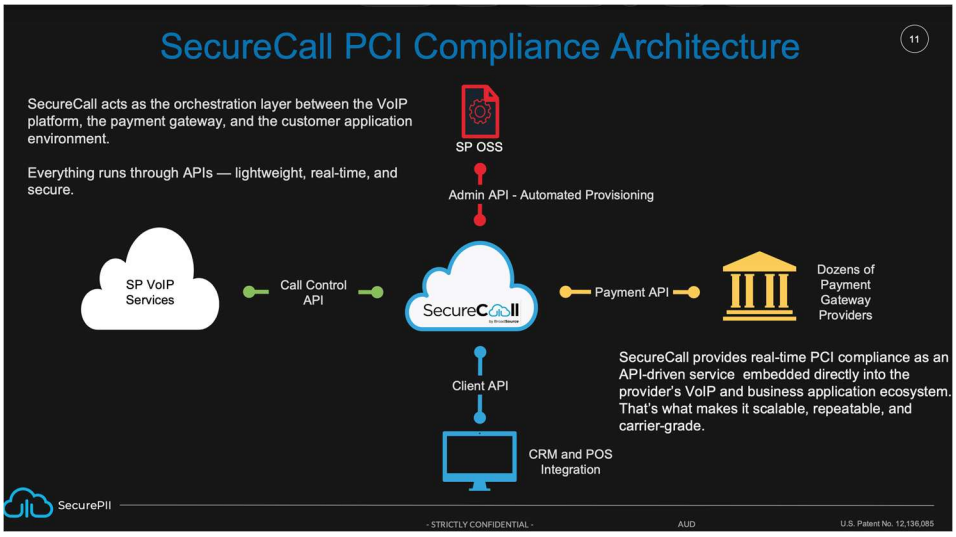
1. Call flow proof and negative evidence: CHD, PAN and SAD never traverse enterprise endpoints, recording, or storage.
2. TPSP evidence: AOC and scoped service description, plus a responsibility matrix.
3. Enterprise still maintains security awareness and TPSP management, but the deep testing of agent workstations, recording platforms, and VoIP path is reduced because the payment data is not present there.

The Modern Solution for Voice-Based PCI Segmentation

Modern PCI compliance requires eliminating CHD and SAD from merchant and enterprise systems before it arrives. The goal is to descope as much of the enterprise as possible by, in essence, descoping the enterprise from PCI Compliance; or, put differently, outsourcing the PCI Compliance function. Traditional pause/resume systems, agent scripting, and manual muting are insufficient, overly costly, error prone or outdated due to technical debt. It is important to remember, as established above, that the entire physical environment is "in scope" for PCI Compliance when CHD is spoken over the phone.

A modern voice-segmentation boundary must:

- Isolate CHD from the voice stream.
- Prevent CHD from entering merchant audio, desktops, recordings, or logs.
- Allow agent to remain on the call.
- Support AI/LLM redaction and safe analytics.
- Align with PCI-DSS scoping rules.
- Work across call centers, retail stores, and multi-location enterprises.



SecurePII's *SecureCall PCI Compliance* ***cloud is accredited at the highest level of compliance with the Payment Card Industry Data Security Standard,*** Level 1 PCI DSS **S**ervice **P**rovider**, and** removes cardholder data **input by phone** from the merchant environment during telephone payments **and/or card tokenization** by inserting a just in time, on demand, secure cardholder data environment into an active call. Instead of relying on procedural controls such as pause and resume, SecureCall uses UCaaS call control APIs and a pre-integrated SIP trunk to temporarily join the SecureCall application to the live call outside the enterprise environment and into the SecureCall cloud.

When SecureCall is invoked, the customer and agent remain on the same call, but card entry is performed by the customer using the dial pad on the phone they called on, and by inputting the credit card numbers, expiration date and CVC. The tones (called "DTMF" Dual-Tone Multi Frequency") are terminated inside SecureCall's PCI DSS Tier 1 Service Provider validated environment, and masked before they reach the agent, and never traverse the enterprise voice network, desktops, recording systems, or storage platforms. As a result, agents do not hear, see, or handle CHD or PAN, and the enterprise telephony, endpoints, and recordings can be materially and substantially de-scoped from the PCI-DSS 4.0 requirements.

From a PCI perspective, SecureCall directly addresses the core issue highlighted in PCI SSC guidance and DSS 4.0 Section 2.3: spoken card data places people, process, and technology into scope. SecureCall is an architecture solution that eliminates spoken CHD, PAN and SAD, rather than attempting to manage that risk procedurally. Architectural solutions scale far more effectively than policy prescriptions and compliance videos. Using SecureCall, the outcome is reduced scope, reduced reliance on human controls, elimination of sensitive authentication data from call recordings, and a clearer, more defensible CDE boundary for any Qualified Security Assessor or Internal Security Assessor to review.

Conclusion

The voice channel remains one of the most misunderstood elements of PCI-DSS 4.0 compliance. Manual card entry from spoken card data places full PCI scope on merchant environments across industries. Merchants cannot rely on component certifications to achieve PCI compliance. Modern architectural solutions permit segmentation to prevent CHD, PAN, and SAD from entering enterprise and merchant systems. This paper provides the foundation for correcting market misunderstandings and outlining effective architectural solutions that enable businesses to scale at the speed of AI as compared to policies and compliance checks.