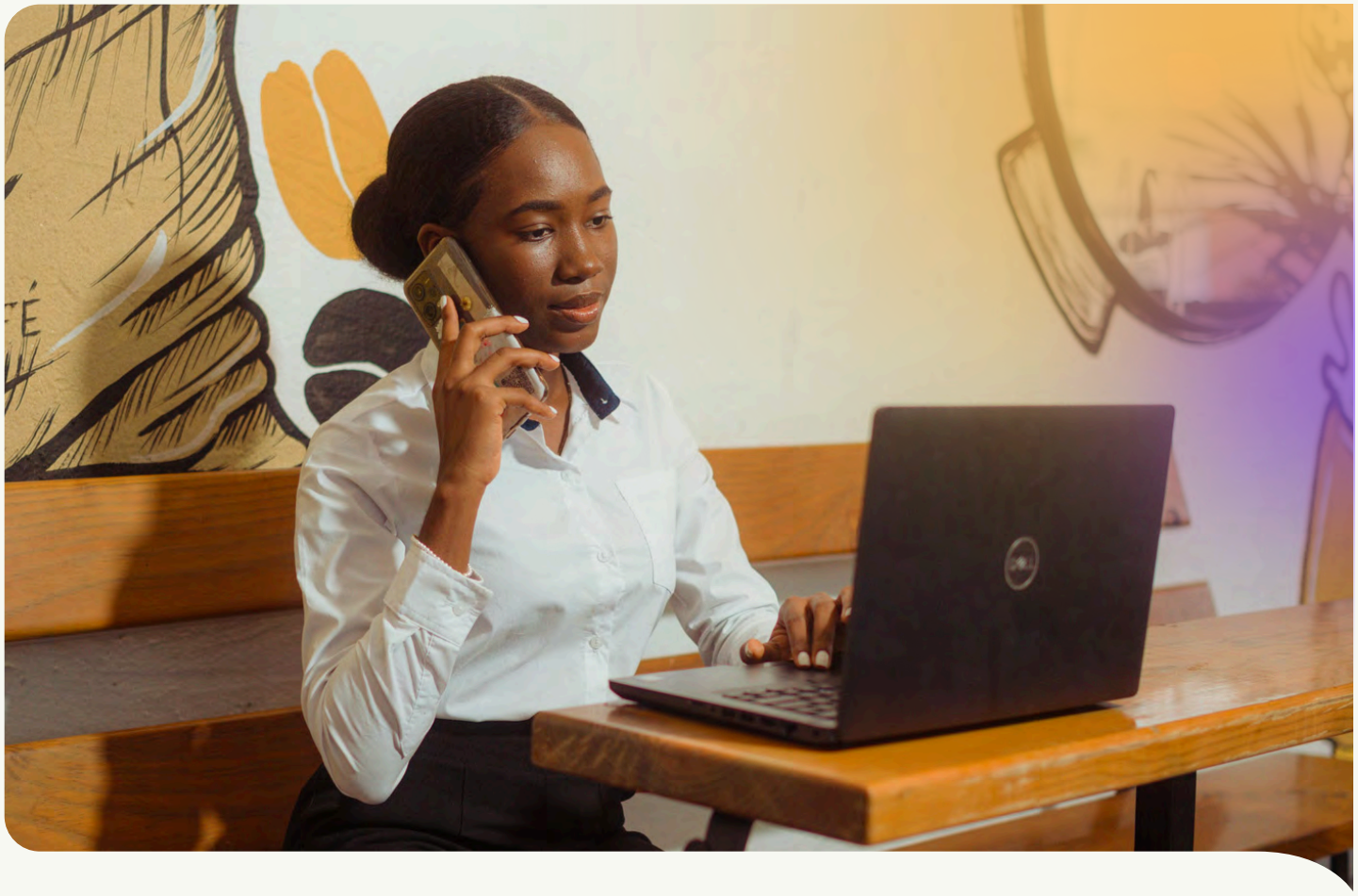
Sharpen

Buyer's Guide



The 2026 Buyer's Guide **to Secure Pay-by-Phone Payment Capture**

A Practical Framework for Regulated Industries

Secure Phone Payments as Core Infrastructure

Mobile is the leading preferred bill-pay channel in the United States. At the same time, a significant segment of customers continues to complete transactions over the phone — particularly in regulated, high-volume environments such as utilities, healthcare billing, financial services, and essential services.

In one utilities and telecom study, only one quarter of consumers reported using their provider's IVR. Yet among those IVR users, two-thirds used it specifically to pay bills. When customers reach the voice channel, they transact.

Organizations processing large volumes of payments over the phone face a structural reality: the voice channel carries financial, operational, and compliance weight. The question is not whether customers should be calling — it is whether the payment architecture behind that call is properly designed.

This guide focuses specifically on secure self-service IVR/IVA payment capture powered by Plum. It outlines the architectural decisions, input method tradeoffs, and procurement considerations that matter most in 2026.

What Buyers Get Wrong About Secure Voice Payments

Across regulated industries, the same misunderstandings surface during payment modernization efforts.

"AI Voice Agents Can Take the Payment."

AI voice systems are built for intent capture, routing, and conversational automation. Most are not PCI environments designed to securely capture and process primary account numbers (PAN) or CVV data.

Secure payment capture requires a dedicated PCI-compliant IVR environment. Voice systems should trigger payment workflows — not process card data directly. Blurring that boundary expands PCI scope and increases audit complexity.

"Self-Service Automatically Reduces Risk."

Self-service changes who collects the data — not where the data flows. If card data passes through call recordings, QA archives, agent desktops, or non-segmented infrastructure, exposure remains. Risk is determined by containment architecture, not by the absence of a live agent.

"Speech Input Should Replace Keypad Entry."

Speech recognition improves navigation and intent detection. For long numeric strings such as card numbers, keypad (DTMF) entry provides control, accuracy, and predictable handling of sensitive financial data. Effective payment systems use speech and keypad input deliberately based on function — not trend.

"Voice Payments Don't Require Strategic Attention."

Voice transactions represent high-intent interactions. Customers calling to make payments are ready to transact. Under-designed IVR systems create friction, increase retries and divert volume to agents. Properly architected payment flows reduce friction while maintaining compliance integrity.

Executive Insight: Voice as Transaction Channel

Customers who reach the phone channel often do so with urgency — pending shutoffs, billing questions, time-sensitive obligations, or account corrections. The architecture behind that interaction directly impacts revenue capture, compliance exposure, and operational efficiency.

How Secure Self-Service IVR Payments Should Be Architected

Secure voice payment systems are controlled PCI environments intentionally separated from broader contact center infrastructure.

In a properly designed architecture:

- Payment capture occurs inside a dedicated PCI-compliant IVR environment.
- Card data is not stored in call recordings or QA systems.
- Sensitive input is isolated from agent desktops and CRM interfaces.
- Payment data routes directly to the processor.
- Tokenization prevents long-term storage of raw cardholder data.

Containment reduces PCI scope and simplifies compliance oversight.

DTMF vs Voice/ML: Functional Tradeoffs

Modern secure IVR platforms support both keypad (DTMF) and Voice/ML input. For sensitive numeric data such as card numbers:

- Keypad entry offers predictable digit capture.
- It avoids callers speaking financial data aloud.
- It aligns with established PCI handling guidance.

Voice/ML input is well suited to navigation, account lookup, and conversational routing.
Design decisions should align with risk tolerance, call environment, and transaction complexity.

Executive Insight: PCI Scope Expands Through Integration

PCI exposure in voice environments typically expands through system integration — not a single failure. Common expansion points include:

- Call recording systems
- QA archives
- Agent desktop visibility
- Internal logging tools

Architectural separation between conversational systems and payment environments prevents scope creep and reduces long-term audit burden.

AI Voice Agents and Secure IVR Handoff

AI voice agents increasingly manage routing and conversational automation. Secure payment capture should occur within a PCI-compliant IVR environment.

In a modern architecture:

- The voice system identifies payment intent.
- The interaction is transferred to a secure IVR workflow.
- Payment data is captured within the PCI environment.
- The transaction is processed.
- Confirmation is returned without exposing cardholder data.

This separation preserves conversational intelligence while isolating financial data inside a hardened payment environment.

Executive Insight: Accessibility and Channel Choice

- Payment strategy is not about replacing channels. It is about designing each channel appropriately.
- Mobile, web, and voice each serve distinct customer behaviors and environments. Secure voice payment capture supports customers who choose — or require — the phone channel for financial transactions.

Questions Procurement Should Ask

→ Is payment capture fully contained within a dedicated PCI environment?

→ Does card data ever pass through call recordings or agent desktops?

→ Is tokenization applied immediately upon capture?

→ How are AI voice systems segmented from PCI workflows?

→ Can input methods (DTMF and Voice/ML) be configured by use case?

→ How does this architecture reduce PCI scope relative to agent-assisted capture?

Conclusion: The Architecture is the decision

Organizations that treat voice payment infrastructure as an afterthought tend to discover its importance during an audit, a breach, or a customer complaint. The organizations that get it right build the payment environment deliberately — segmented, compliant, and designed for the transaction volume it will actually carry.

AI is changing how customers interact with contact centers. It is not changing what secure payment capture requires. The fundamentals — containment, tokenization, PCI scope reduction — apply regardless of how sophisticated the conversational layer becomes.

The questions in the preceding section are a starting point. The answers will tell you whether your current architecture is built for what your customers actually need from the voice channel.

About Sharpen

SharpenCX is a customer experience platform designed for organizations where service, security, and compliance matter. The cloud-native solution integrates contact center operations, AI-enabled automation, and secure voice payment capabilities to help teams resolve complex customer interactions with confidence. SharpenCX supports regulated and high-stakes industries — including utilities, healthcare, and insurance — where reliability and risk reduction are essential.