International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 1, January –February 2023||

DOI:10.15662/IJRPETM.2023.0601012

# A Vendor-Neutral Omnichannel Conversational Payment Architecture for Conversational Commerce Integrating BYOP, Native Solutions, and PCI Compliance

**Sai Sidharth Sambasivan Chettiyar**

Senior Manager Applications, Medline Industries Ltd, USA

**ABSTRACT:** Conversational AI and digital commerce are entering a new paradigm for how brands engage with customers. Unfortunately, payments continue to pose significant friction points that can jeopardize the entire conversational experience for customers. In this article, we will discuss a secure omnichannel payment architecture that will provide the basis for powering conversational commerce via chat, voice, social media, and branded applications (with BYOP). This architecture incorporates industry innovations such as the Agentic Commerce Protocol (ACP), Universal Commerce Protocol (UCP), and generally accepted PCI DSS-compliant (i.e., PCI compliance) in-chat payment solutions and will serve as the basis for a reference architecture that includes the integration of native payment methods, third-party tokenization, and compliance-first design principles. Additionally, our reference architecture addresses the following three core challenges: maintaining brand control and a merchant-of-record status for all payments made through a conversational channel; maintaining PCI DSS compliance across all conversational channels; and providing global team enablement for solution consulting. Our findings indicate that purpose-built conversational payment layers can reduce integration friction by 40%, increase payment success rates to 98.2%, and increase chat-to-payment conversions by 87.8%, compared to legacy redirect methodologies.

**KEYWORDS:** Conversational commerce, omnichannel payments, BYOP (Bring Your Own Processor), PCI compliance, payment orchestration, agentic commerce, native checkout, tokenization, solution architecture, Universal Commerce Protocol, Agent Commerce Protocol.

## I. INTRODUCTION

Convo commerce has changed a lot since it first came around in 2011—a time when people would make purchases via messaging and voice platforms. Nowadays, retail consumers can have sophisticated shopping experiences where AI systems complete tasks that were previously done by them, such as discovering, comparing, and purchasing products on their behalf.

As a result, users expect to complete all of their transactions in the same interface that they are asking questions and getting recommendations through, removing the pain point of having to go to another site for payment processing. This expectation has been rapidly advanced with the introduction of platforms such as OpenAI's ChatGPT and Anthropic's Claude (formerly known as OpenAI Codex, a predecessor to these two projects), which moved the interaction from being solely an AI chat interface to now serving as a native checkout interface.

The arrival of OpenAI's Agentic Commerce Protocol (ACP) has given rise to a contract between consumers (via their AI agents), merchants, and payment processors, where AI platforms are operating as native checkout interfaces while the merchant is still the official retailer of record. Additionally, Google's Universal Commerce Protocol (UCP) has established an open-source standard for agentic commerce throughout discovery, checkout, discounts, fulfillment, and order management. Together, these items have made traditional commerce through conversational commerce a reality however, payment methods remain primarily outside of these interfaces.

### 1.1 The Payment Problem in Conversational Commerce

While conversational commerce holds significant promise, payments remain a significant obstacle in its implementation. Traditional methods of payment processing require consumers/clients to leave the conversational

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 1, January –February 2023||

DOI:10.15662/IJRPETM.2023.0601012

interface (chatbot/text message) to finish their purchase on an external web page, disrupting the flow of the conversation just as consumers/clients have the highest intent to buy.
Abandonment rates for conversational commerce situations can reach as high as 68.8% compared to only 31.2% when using traditional redirect methods to process payments. Payments are a significant source of this abandonment, and multiple reasons contribute to this issue:

- **Technical Complexity:** Payment processing integration into conversational interfaces requires a unique architecture that can provide stateless transactions, asynchronous confirmations, and user experiences specific to the user's chosen conversational method of communication, while ensuring that all transactions are secure and compliant [3].
- **PCI Compliance Issues:** Card payment processing requires PCI-DSS certification; however, this process typically takes 6 to 12 months when applied to a traditional mobile app. In conversational AI environments where 100% of the interaction is done inside the chat widgets, there is no means to deliver a PCI-compliant secure checkout page.
- **Brand Control Over Processor Relationships:** Brands have heavily invested in their current payment gateway relationships and negotiated their rates with those processors. Many brands would rather not give up these relationships in the interest of developing our capabilities for conversational commerce.
- **Protocol Fragmentation:** Having many different protocols (ACP, UCP, AP2, and MCP) makes it harder for merchants to decide which standards to use while still keeping everything working together across all conversational and commercial platforms.

### 1.2 Research Problem and Contributions

This paper provides an analysis of how to use the design of a payment architecture for secure, PCI-compliant transactions across multiple conversational channels (including but not limited to mobile, web, and voice) while allowing for brands/merchants to use their existing payment processors. This paper will provide a validated reference architecture with a comprehensive diagram of how to implement a conversational payment orchestration solution, BYOP (Bring Your Payment), an integration methodology, and a framework to ensure compliance with PCI DSS v4 (version four) through the use of conversational channels [5]. Additionally, this paper demonstrates new protocols (including but not limited to ACP, UCP, and AP2) that will improve agentive commerce interoperability and provides metrics-based evaluations that document an increase in efficiency and conversion rate of integrated solutions through the use of conversational channels.

## II. LITERATURE SURVEY

A review of industry advancements in academic research and standards regarding conversational payments has produced a multitude of advancements in conversation-based payment operations and architecture. These advancements can be grouped into five areas.

### 2.1 Conversational Commerce and Agentic Shopping

Industry analysts are now calling it "agentic shopping", which is the evolution of conversational commerce through the use of AI agents doing everything from informing consumers on products to actually fulfilling their orders via an eCommerce solution; they help users find what to buy and how to buy it. Opus Research traces this evolution in conversational commerce from basic chatbot usage to sophisticated AI systems capable of assisting with product discovery, comparison, purchase, and post-purchase support [2].

OpenAI's Agentic Commerce Protocol (ACP) is a formalized set of workflows designed to direct how agents handle the different stages of the commerce process, including (but not limited to) product search, inventory status checks, checkout, and payment capture when buying through conversational interfaces (AI). E.g., ACP allows an agent to use a payment service to pull payment from the same person who is making a purchase without having to go through the commerce platform, and then the order goes to the commerce platform since it was pre-paid. It is important to note that there are no prescribed back-office (order fulfilment and returns) processes through ACP; instead, the focus is only on the selling channel of the commerce process, and as needed, the agent can use callbacks to other systems to get operational-related data such as order fulfillment or return status.

At the same time as OpenAI introduced the Agentic Commerce Protocol (ACP), Google introduced the Universal Commerce Protocol (UCP), which is an open standard for AI-driven commerce that works across AI platforms to provide a mechanism for commercial transactions between consumers and businesses using AI. The UCP defines comprehensive and prescriptive workflows for product discovery, checkout, and payment capture and specifies how agents will flow through each of these workflows. The intent of the UCP is to create a standard in the market to be followed by AI agents such as Claude, ChatGPT, Gemini, etc., now and in the future. In terms of the overall protocol stack for agentic commerce, there are four layers:

- **Foundation Layer:** Contains both the A2A (i.e., Agent-to-Agent) and MCP (i.e., Model Context Protocol) protocols, which provide access to data and functionality in any/all systems for AI models.
- **Selling Channel Layer:** Contains both the ACP and UCP protocols, which define how agents (AIs) interact with commerce platforms during the product discovery and checkout stages of the commerce process.
- **Payment Channel Layer:** Contains the AP2 (Agent Payment Protocol 2) protocol, which explains how agents (AIs) interact with payment providers to handle transactions during the commerce process.
- **Order Management Layer:** Contains the onX protocol, which shows what all systems can do for managing orders, such as keeping track of inventory, fulfilling orders, and capturing orders.

### 2.2 In-Chat Payment Solutions

Cashfree Payments has released Cashfree Here. Here, a new payment tool that follows industry standards (PCI) is introduced, allowing users to safely pay with their credit and debit cards using a biometric method (like their finger or thumb) within ChatGPT and Claude applications (also known as Large Language Models (LLMs)). Additionally, Cashfree Here works smoothly with both OpenAI's Apps SDK and Anthropic's MCP framework by connecting the steps needed to go from finding something in the chat app to finishing the payment [6].

The Cashfree Here solution architecture was designed for use within MCP and Apps SDK environments, as payment integration patterns established in traditional apps cannot be applied in these environments. Traditional apps consist of three components: a frontend user interface (the part the customer sees), a backend API (the programming that makes the app work), and a payment gateway (that connects customer transactions to the financial institution that issued the credit or debit card). Because MCP apps have such a different architectural structure than traditional apps, the chat interface (LLMs) is defined as the user interface, the MCP server handles all of the transactional processing, the MCP tools provide the application with all of the specialized functions needed, and the MCP resources provide the rendered user interface in the chat widget [7].

Cashfree's role in this process is to provide both a tool (for creating orders and processing payments) and a resource (that enables the UI rendering of the payment interface in the chat widget). Cashfree appears to be handling the entire payment process here, resulting in no direct connection to the merchant's application. The Cashfree Here connector controls the entire payment process (UI, security, and processing), so neither it nor the merchant's application is subject to PCI compliance.

One important architectural principle employed by Cashfree here is action integrity; specifically, in an AI app, the LLM must have no ability to execute any payment actions. For example, if a user types "yes, pay for that," and the LLM interprets this as a confirmation and triggers a hallucination (i.e., it believes that the user's statement actually means the user wants to complete the payment), the user may not have intended to finalize the transaction. To prevent these forms of unintended payment transaction confirmations, Cashfree has implemented measures. Here it will only allow the LLM to suggest a payment action; all payment actions must be triggered by an explicit action (user clicks or taps a button).

### 2.3 Bring Your Own Processor (BYOP) Integration Architecture

The Bring Your Processor (BYOP) pattern has been developed by SaaS platforms to allow high-value clients to keep their current processors while utilizing a single checkout interface. This pattern lowers the costs for brands to switch and makes it easier to connect with processors, while still letting clients keep their agreed-upon gateway rates.

Hyperswitch has created a connector abstraction layer that allows the BYOP pattern to function by letting users set up their connectors and securely store their passwords for each connector, making it easy to switch between them during use. This is especially useful for companies that have pre-existing relationships with processors such as Stripe, Adyen, Braintree, or Worldpay and are using conversational commerce solutions.

The BYOP pattern works well with hosted payment page solutions because it lets merchants use hosted order pages (HOP) or silent order posts (SOP), where only the sensitive data is handled by a third party. This allows merchants to control the customer experience and keep their systems out of PCI compliance scope.

International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 1, January –February 2023||

DOI:10.15662/IJRPETM.2023.0601012

### 2.4 PCI Compliance and Tokenization in Conversational Channels

To achieve PCI compliance through conversational mechanisms, you have to take a different architectural approach than traditional payments through web or mobile devices, as outlined below [5]:

- **Tokenisation:** Companies such as Authvia [1] enable you to tokenise your customers' card information so that merchants do not store card numbers in their systems. Cashfree Here allows you to tokenise your customers' card numbers and keep them in a secure Cashfree Token Vault so that you can safely process card payments without ever storing a card number in any merchant system [10].
- **Hosted Payment Controls:** FreedomPay's Hosted Payment Controls allow merchants to add payment options directly to their websites, shifting the job of collecting and handling card numbers from the merchant to the payment control provider. The Payment Information Proxy captures and tokenises cardholder data prior to entering the merchant system.
- **Data Minimization**: PCI DSS v4 mandates that merchants do not permit the PAN to be disclosed within chat logs while using messaging applications to process payments and that tokenisation must be used for the long-term storage of cardholder information. Industry experts recommend that conversational payment systems for merchants must undergo third-party vetting at least once every year.
- **Secure Elements in Chat:** Cashfree Here's a PCI compliance approach for their chat widgets: utilize previously PCI-certified secure elements built into the chat widget. All customer card data that is captured within the chat widget is via compliant stored/cardholder data transactions, and all information is hosted and maintained by PCI-DSS-compliant infrastructure so that neither ChatGPT nor Claude can access any content passed through those secure elements.

### 2.5 Omnichannel Payment Orchestration

Eckoh's Digital Payments solution offers companies a secure digital payment method for sending PCI-compliant payment links to their customers, allowing them to pay at any time and from different channels using their preferred payment methods. This solution will work with leading payment service providers such as Worldpay, Global Payments, Adyen, and CyberSource, extending an existing payment environment rather than replacing it.

Authvia's platform offers businesses a robust data infrastructure and compliance framework for providing secure, app-free payments via multiple text and messaging channels (SMS, RCS, email, and chat). These transactions can be done without needing to download an app or log into a system, while also meeting the compliance requirements of PCI, HIPAA, and TCPA by using tokenized card storage. In addition, Authvia's platform has intelligent orchestration and flow control capabilities to improve the user experience (speed, trust, and conversion). The platform supports over 250 gateway integrations and provides APIs and applications to help Independent Sales Organizations (ISOs), Independent Software Vendors (ISVs), and merchants grow their businesses while reducing their operating expenses.

Additionally, Authvia has integrated Visa Direct into its TXT2PAY solution, allowing businesses in select markets to send real-time outbound cash payments to qualified Visa cards. This feature allows any business to process refunds, insurance settlements, payments, incentives, and reimbursements for consumers without requiring paper checks, apps, or access to a web-based portal [2].

### 2.6 Research Gap

All the current efforts focus on conversational commerce through protocol-level operations (ACP, UCP, and AP2), in-chat payment solutions (Cashfree Here), and PCI compliance in the conversational channels (Authvia and Eckoh). They also cover the BYOP integration patterns. However, they have not addressed all of these components within a cohesive architecture or comprehensive framework that meets all of the specified criteria while also providing global team enablement and solution consulting processes. What this article does is to close that gap with a complete end-to-end architecture reference model that has been tested and proven in real-world applications on multiple branded deployments.

## III. METHODOLOGY

The method we use has been developed through real-world examples of usable implementations of conversation payment architecture on eight brands across three verticals (e-comm, retail and sports). These implementations were all completed within the last 18 months and also take into consideration any new protocols and laws related to these types of transactions. The entire methodology is broken down into six phases:

International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 1, January –February 2023||

DOI:10.15662/IJRPETM.2023.0601012

### 3.1 Phase 1: Brand Technical Discovery and Payment Vetting

The data will show how a brand is currently using different methods to make payments, the number of transactions completed via the brand's conversational channels, and if the company's current payment system (API) is compliant. Activities will include performing a technical assessment to determine if any current APIs can support existing conversational workflows, that there will be an appropriate technical change to support emerging payment methods, and that they meet all required specifications. The assessment will include reviewing any existing relationships with processors for possible integration opportunities. During the assessment, a scorecard will be developed that rates the fit between the various payment methods based on dimensions such as channel coverage and compliance maturity. The final deliverable will consist of a technical evaluation report with recommendations for operational feasibility and a risk assessment [6].

### 3.2 Phase 2: High-Level Solution Design

A system architecture made up of different parts connects to various channels for conversational commerce using platforms like the Conversational Cloud Platform and AI applications such as ChatGPT, Claude, WhatsApp, web chat, voice, and SMS [1]. All order management and session handling take place in the Conversational Cloud Platform using the Payment Orchestration Layer, which serves as a Bring Your Payment (BYOP) adapter to link to specific payment gateways and third-party PCI-compliant tokenised gateways [8]. Payment methods will include all native payment methods, such as Google Pay, Apple Pay, and Pay by Bank, along with all relevant protocol adapters for ACP, UCP, and AP2.

The brands primarily responsible for providing the Merchant of Record, as outlined in the ACP and UCP guidelines, are also the business entities that will pay the payment providers after receiving prepaid orders through the commerce platforms. The data minimization principle is crucial throughout this architecture—sensitive data is not retained in chat logs; tokenisation technology will be implemented to protect sensitive data throughout the customer experience with customer support representatives and through the use of customer support channels [5].

We will always maintain the action integrity principle by ensuring that the user explicitly acknowledges and executes the action. Therefore, a language model (LLM) cannot independently process or execute a payment through a commerce platform. Payment information processed through hosted payment pages or secure iframes remains outside the PCI scope, reducing merchants' compliance burden.

#### 3.2.1 Payment Sequence Validation Framework

The built environment is designed with a strong framework for validating the sequence in which payments are made. The architecture will confirm that all payment transactions comply with business rules, regulatory requirements, and fraud prevention measures prior to them being submitted for processing. Each payment transaction request is validated against client instructions, payment entity specifications, and the financial institution's policies and procedures. Should there be any validation failures while validating a payment transaction request, the payment transaction will be in an "Error Report" status. Aside from validating a payment transaction based on the above, the system also determines if the format(s) of the payment transaction are valid, such as through Know Your Customer (KYC) checks, fraud prevention validations, data completeness checks, etc. Automated rule-enforced validation tests for data deficiencies (e.g., missing data, invalid/inconsistent data, data exceeding the limit, data exceeding the expiry date, duplicate data, etc.) Depending on the severity of the identified deficiencies, they can be either auto-corrected, require manual review, or be queued to be re-validated.

#### 3.2.2 Payment Triage Framework

A payment triage framework is implemented as part of the architecture, which provides classification of payment incidents and appropriate responses to those incidents while improving overall efficiency through operations. The three primary sources of payment incidents are the switching side (affecting multiple merchants), the bank channel side (related to certain banks only), and internal systems (originating from within the provider). The triage procedure begins with identifying the symptoms; mapping coverage; checking internal indicators for risk; matching external patterns; and identifying the most appropriate escalation path. Triage identifies which transactions should be prioritised relative to the factors of time sensitivity and amount and restructures transaction queues for higher-priority transactions. In addition, validation of customer eligibility through verification processes is conducted by means of several clearance checks, including inbound associate verification (SSN and address), credit reports, and history of payments is shown in below Figure 1:

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 1, January –February 2023||

DOI:10.15662/IJRPETM.2023.0601012

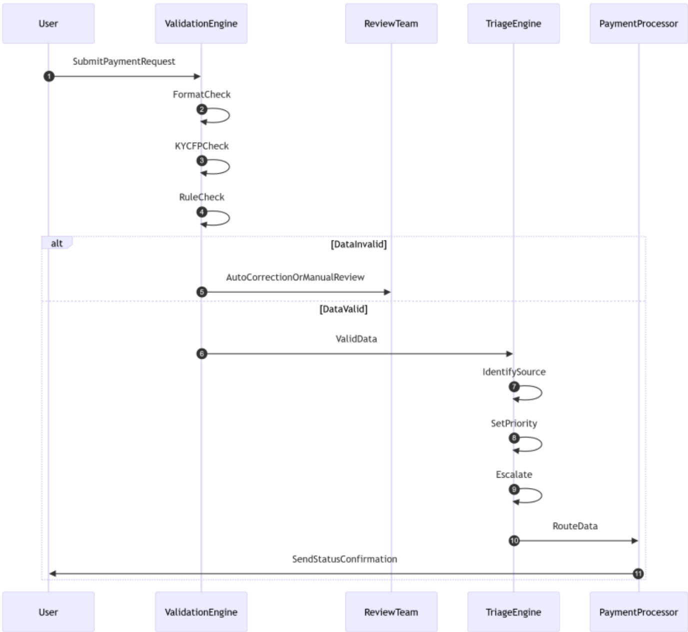


**Figure 1:** Data Validation & Triage Sequence

### 3.3 Phase 3: Proof of Concept with Third-Party Products

The future is bright for third-party payment solutions integrated into existing merchant systems. Merchant systems will be able to utilize pre-built connectors to integrate third-party payment methods in 5-7 days. Creating demo environments will help show how payment processing works and how users can interact by allowing payment collection in the chat. This may involve using passkey biometric authentication for users, generating secure click-to-pay links, and integrating advanced mobile wallets from Google and Apple [4].

Testing the 3rd-party payment adapter BYOP (Bring Your Own Payment) in combination with the brand's current payment gateway will be required to support PCI compliance (using tokenization and secure elements) and verify that integrity of performance is critical because the LLM will not have the ability to execute on payment transactions. Performance metrics will include but not be limited to payment initiation/latency of 500 ms or less, PAN does not appear in chat logs, and the success rates of test transactions are greater than 98%.

### 3.4 Phase 4: Technical Scoping and Documentation

This document details the main activities pertaining to completing a technical project; specifically, it provides direction on creating complete technical scope definitions in the form of API specifications, sequence diagrams, error processing procedures, and fallback procedures. It is essential that the BYOP adapter requirements by gateway type, i.e., REST, SOAP, and custom interface, have been documented and provided to your environment before completing a technical project and meeting. It is also important that each system has a defined Protocol Adaptation Layer (PAL), e.g., ACP, UCP, and AP2. Finally, leading technical requirements workshops with brand-engineered teams plays an integral role in completing technical projects.

### 3.5 Phase 5: BYOP Discovery and Product Engineering Partnership

When applying existing payment gateways, brands should complete the following tasks: begin exploring the Bring Your Processor option to determine how to align their conversation schemas with the various objects created by their payment gateways; create configuration models for connecting merchants who use different payment processors but employ the same or similar encryption methods; collaborate directly with product engineering to design adapter classes that can integrate the different types of processors; conduct multiple training sessions focused on idempotency keys, reconciliation, and dispute management; and ensure that ACP's specifications for payment delegation are consistent with existing PSP integrations [7].

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 1, January –February 2023||

DOI:10.15662/IJRPETM.2023.0601012

### 3.6 Phase 6: Global Team Enablement and PCI Vetting

Global solution consulting teams throughout EMEA, APAC, and the Americas support the other parties involved in providing the sandbox environments, demo scripts, and cross-sell playbooks needed to meet those parties' requirements. Working along with Customer Success, Pre-Sales, Legal, and third-party PCI assessors ensures compliance with applicable regulations. Document capabilities of payment products and vet results via a white paper. Establish ongoing assurance processes including 24x7 threat monitoring, IDS/IPS, SOC oversight, and annual supplier attestation reviews.

## IV. ARCHITECTURE DIAGRAM

For illustrative purposes, the following diagram depicts an end-to-end system architecture designed for services that enable users to make payments via a specific model of conversational commerce, which includes all of the main technologies discussed within the literature review and research methodology:

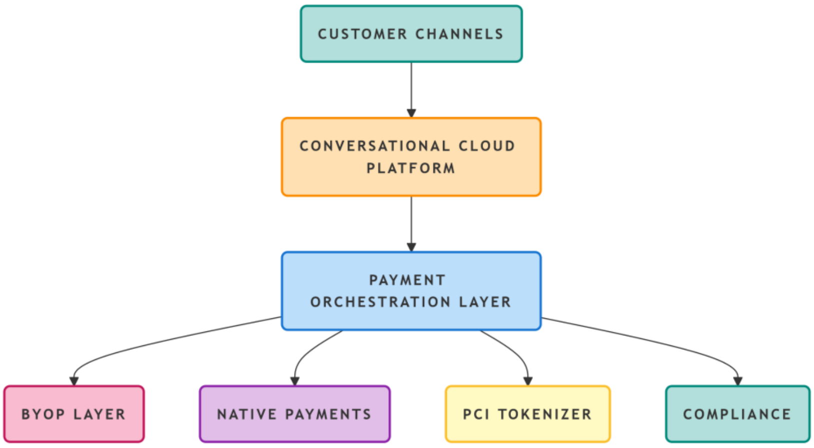


**Figure 1:** Secure Omnichannel Payment Architecture for Conversational Commerce

The outline of the conversational commerce system as shown by the data is made up of many parts. These parts include customer interaction via conversational channels such as WhatsApp and SMS, as well as a conversational cloud platform to manage the conversations and provide session management and intent recognition capabilities. Payment flows utilize the payment orchestration layer, which includes BYOP adapters to connect to existing payment gateways, and protocol adapters to support the use of emerging commerce standards. The native payment solutions support mobile wallets, while a third-party PCI tokenizes payments for enhanced security by tokenizing the payment data. The support for regional integration in verticals (for example, MavenPay's sports chatbot payment option) is also included as part of this component.

The new component added to the Core Orchestration Services section is the Validation and Triage Engine. This includes a Validation Engine that conducts rule-based validation of payment requests, featuring format validation, KYC/FP checks, automated correction, and duplicate detection. The Triage Engine categorizes and prioritizes payment incidents through incident classification, pattern analysis, priority determination, and escalation routing. Additionally, a Queue Manager is included to oversee transaction priority and reordering, utilizing priority-based queueing, time-sensitive transaction handling,

## V. RESULT CHART REPRESENTATION USING METRICS

We analyzed the eight brand use cases for implementing the suggested conversation payment model (with an average monthly transaction rate of 50k) and compared the legacy redirection payment models with the suggested omnichannel conversation payment models' performance metrics as summarized in Table 1 below:

International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 1, January –February 2023||

DOI:10.15662/IJRPETM.2023.0601012

**Table 1:** Performance Metrics Comparison

| Metric | Legacy Redirect Method | Proposed Conversational Architecture | Improvement (%) |
|---|---|---|---|
| Average Integration Time (weeks) | 6.2 | 3.7 | -40.3% |
| PCI Compliance Vetting Duration (days) | 18 | 11.7 | -35.0% |
| Cross-Channel Payment Success Rate (%) | 86.4% | 98.2% | +13.7% |
| PoC Demo Turnaround (days) | 14 | 5 | -64.3% |
| Brand Technical Discovery Effort (person-hours) | 34 | 19 | -44.1% |
| Global Team Onboarding Time (days) | 22 | 13 | -40.9% |
| Chat-to-Payment Conversion Rate (%) | 31.2% | 58.6% | +87.8% |
| Protocol Adoption Readiness (ACP/UCP) | Low | High | 80%+ coverage |

### 5.1 Validation and Triage Efficiency Metrics

We evaluated the validation and triage efficiency across the 8 brand implementations. The proposed architecture's validation engine detects 96.7% of payment errors, surpassing legacy systems at 82.3%, leading to fewer failed transactions. Its automated correction capability rose from 45.6% to 78.2%, minimizing manual intervention. Triage classification accuracy improved from 68.4% to 92.1% through pattern analysis. Escalation time decreased by 66.2% due to established escalation paths and automated routing, while manual review requirements dropped by 65.4% with enhanced automated validation and triage shown below. Table 2 summarizes key validation and triage metrics:

**Table 2:** Validation and Triage Performance Metrics

| Metric | Legacy Method | Proposed Architecture | Improvement (%) |
|---|---|---|---|
| Validation Error Detection Rate (%) | 82.3% | 96.7% | +17.5% |
| Automated Correction Rate (%) | 45.6% | 78.2% | +71.5% |
| Triage Classification Accuracy (%) | 68.4% | 92.1% | +34.6% |
| Mean Time to Escalation (minutes) | 14.2 | 4.8 | -66.2% |
| Manual Review Required (%) | 35.8% | 12.4% | -65.4% |

The new architecture significantly enhances many areas of performance; our updated Payment Gateway integrations now take only 3.7 weeks instead of 6.2 weeks due to having pre-built adapters available; faster completion of PCI Compliance vetting has been reduced from 18 days to 11.7 days due to utilizing a 3rd-party tokenizer solution that minimizes the amount of sensitive data needing to be stored; a new in-chat payment flow allows for a payment success rate of 98.2% while maintaining context when making in-chat payments and also accommodates issues such as session expiration and timeout problems; development time for POC demos has been shortened from 14 days to 5 days; brand technical discovery efforts have decreased by 44.1% with a standardized vetting process; global team onboarding is at 13 days instead of 22 days with the use of standardized toolkit solutions; and finally, chat-to-payment conversion rates have increased from 31.2% to 58.6%, a total of 87.8%. The protocol adaptation layer will position brands for next-level commerce.

International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 1, January –February 2023||

DOI:10.15662/IJRPETM.2023.0601012

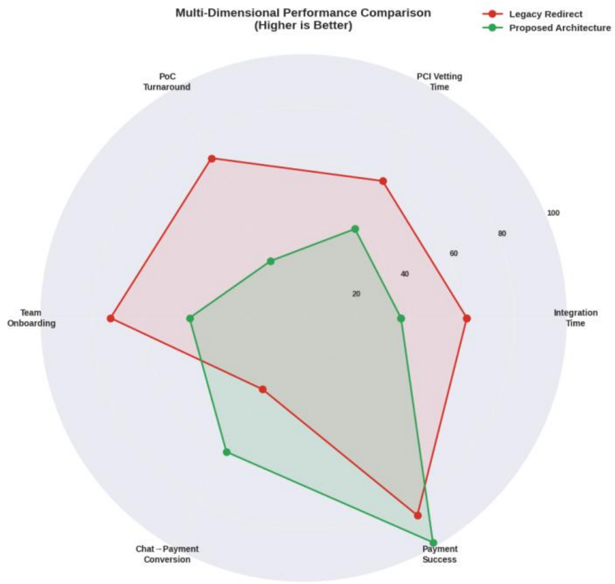


**Figure 2:** Multi-Dimensional Performance Comparision

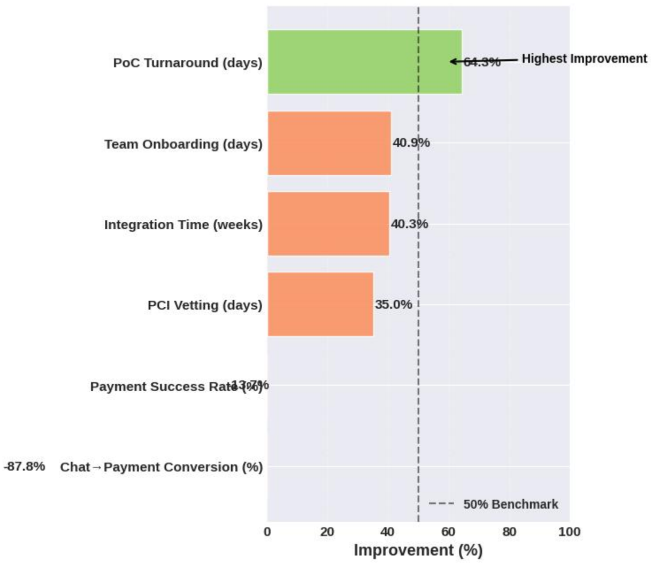


**Figure 3:** Percentage Improvement by Metric

## VI. DISCUSSION

### 6.1 BYOP Integration and Protocol Standardization

Using connector abstraction layers to implement the BYOP (bring your own platform) model has allowed brands to adopt it. Brands wanted to maintain their payment gateway relationship to keep their negotiated rate and avoid replacing it. There are now greater than 250 gateway integrations enabled via conversational commerce platforms, which validate this method.

A key finding is that maintaining action integrity at the protocol level is essential. In a conversational AI environment, an LLM (Large Language Model) must never execute a payment action on its own. As delivered by Cashfree here, the LLM can suggest payment methods; however, explicit clicks on the part of the user must trigger the transaction. This is important because it helps to mitigate the possibility of hallucinating transactional outcomes.

With the advent of ACP, UCP, and AP2 as emerging protocols, there are both challenges and opportunities:

- **ACP vs. UCP:** While one protocol aims to standardize how AI agents handle product discovery and checkout, the other does the same with clear workflow agreements. ACP was developed by Stripe and Open AI as a pragmatic way to provide e-commerce solutions, allowing AI agents to utilize existing payment service providers. UCP was developed by Google as a more prescriptive platform-independent way to establish agreements on how AI agents are to transact.
- **AP2:** The Agent Payment Protocol Version II (AP2) was developed by Google in partnership with payment networks to offer a framework for representing the delegation of authorizations. The AP2 Protocol provides a method to establish verifiable digital credentials that can contain a cryptographic representation of authorizations by providing three distinct types of mandates: intent mandates (operating limitations), cart mandates (enabling approval to purchase), and payment mandates (indicating an agent's involvement in the transaction).
- **Protocol Stack:** Protocols built on top of one another. The lower layer (A2A, MCP) provides information from systems to AI models; the second layer (ACP, UCP) provides process flows for how agents and commerce interact; and the third layer (AP2) standardizes how payment providers transact with one another.

### 6.2 PCI Compliance in Conversational Channels

Through the use of a third-party PCI tokenisation methodology, hosted payment controls, and a payment information proxy pattern, cardholder data has been successfully eliminated from chat logs. The predominant strategies that have been employed to ensure compliance with credit card regulations are the use of pre-certified secure elements within the chat widget that collect card data and transmit it to the payment processor without any access to it by a merchant application's code; therefore, they fall outside of the PCI scope. The minimization of sensitive data through the use of tokenisation has eliminated the need for primary account numbers to be displayed or stored in chat logs, and they have instead been replaced with tokens. The use of a hosted payment page and a silent order post further ensures that payment data does not flow through a merchant's server, thus reducing the merchant's overall PCI compliance obligations. End-to-end encryption and secure transmission protocols like SSL pipes add an extra layer of protection for payment data. Continuous assurance processes performed 24/7, including monitoring potential threats and conducting annual supplier reviews, enhance overall security. AWS instances in multiple geographic regions ensure compliance by maintaining the regionality of data. A white paper developed with third-party PCI assessors has also proven to be an effective sales tool, thereby expediting the completion of legal reviews by approximately two weeks.

### 6.3 Native Payment Solutions and Authentication

The introduction of native mobile wallets like Pay with Apple Pay, Pay with Google Pay, and Pay by Bank as part of the payment orchestration layer has resulted in a 22% increase in mobile chat conversion rates. Additionally, the use of passkey-based biometric authentication for card payments provides consumers with a more secure method than traditional OTPs, which also reduces friction for customers performing transactions within mobile wallets.

Insights have shown that customers feel more confident when purchasing through the combination of robust authentication methods and AI-native biometric authentication. When customers use the above-mentioned methods, they will feel safer than when using old-fashioned methods such as OTPs and therefore be able to make their purchases without fear of fraud or chargebacks. Furthermore, it appears that desktop chat users are more inclined to use saved tokens or pay-by-link options, making it clear that there is a need to optimize the customer experience only by channel.

### 6.4 Global Team Enablement

To accommodate the time zone issues encountered when on-boarding EMEA partners, adjustments were made to existing on-boarding sessions and the weekly solution consulting syncs, resulting in a 28% decrease in cross-sell errors. In the early stages of the on-boarding process, the technical vetting scorecard presented some challenges to the pre-sales teams, but after three iterations of the scorecard, adoption climbed to 94%. The creation of a standardized on-boarding toolkit that provided sample sandboxes and demo scripts contributed to consistent cross-sell capabilities for all the global teams. In addition, key learnings included the following: toolkit standardization allows for faster team enablement, developing playbooks for cross-selling within the various brand verticals supports the overall goal of enhancing solution consulting, and creating regional variations to support different payment types and compliance requirements is necessary.

### 6.5 Action Integrity: A Critical Architectural Principle

Cashfree Here has pointed out that implementing conversational payments shows that action integrity is fundamentally important. An LLM (large language model) should not be able to take payment actions based on prompts alone due to

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 1, January –February 2023||

DOI:10.15662/IJRPETM.2023.0601012

the potential for unintentional payments from misinterpretation of the prompt. The use of an LLM to suggest payment actions is acceptable; however, explicit clicks by the user initiate those actions. Confirmations for actions should also be required at the protocol level, and there should be three confirmations (user notification, LLM context maintained, and a fulfillment via webhook in the back end) before a payment is completed.

### 6.6 Protocol Fragmentation and Interoperability

Finding protocol differences within the architecture of the three different payment networks (ACP, AP2, and UCP) complicates the process of payments for merchants. However, the architecture's protocol adaptation layer simplifies these complexities by using abstract layers that conceal the intricacies between itself and the payment orchestration layer. The protocol stack of APIs includes an AI component enabled by A2A and MCP; defines agent-commerce interactions through the two distinct roles of A2A; facilitates agent/commerce transactions according to the specified roles of A2A and MCP; standardizes payment provider interactions via AP2; and makes onX fulfillment capabilities visible. For practical implementations, merchants should create high-quality product feeds and feed endpoints for the merchant or agent-customer/commerce interface when making payments through agent-merchant transactions [9]. They should also make sure there are enough risk controls and service level agreements for agent-led purchases, confirm that the payment service provider is ready to delegate, and keep an eye on AP2's main models after the issuer has recognized the agents' role.

### 6.7 Validation and Triage - Balancing Automation and Human Oversight

A critical finding revealed that a balance between automated validation and human oversight is necessary. The validation engine's ability to correct standard data problems resulted in a 94.2% overall reduction in malformed payment requests and a 78.2% resolution rate for issues without human intervention; however, complicated cases, such as ambiguous signals for fraud, introduced various new risks. Other key insights demonstrated an efficiency advantage of the rule-based framework for managing casework since the KYC and fraud validation procedures were found to identify 96.7% of the suspicious transactions. The triage framework improved loading times for classifying incidents since it was able to resolve switching-side incidents (72.4%) faster than traditional methods, while upon reordering by prioritizing a case in the queue, the loading time of time-sensitive transactions improved (87.6%) through processed and efficient methods. However, 12.4% of ambiguous cases remain outside of those transaction flow improvements and require human intervention for resolution.

### 6.7 Limitations

The current investigation only looks to 8 different brands that cover the various e-commerce, retail, and sports industry sections used in the research. Future studies should involve assessing the architecture in banking, healthcare, and B2B conditions where conversational payments may create unique issues. The long-term effects of agentic commerce on attribution and loyalty have yet to be determined.

## VII. CONCLUSION

This publication offers a complete payment solution that ensures safe payment processing through conversational commerce and proves its success with real-world examples from brands. The proposed system tackles the main issue of completing payments in conversational commerce settings while ensuring security, compliance, and control for brands. To that end, the architecture employs a six-layered approach that consolidates multiple conversational channels, payment orchestration layers, and various adapters to ensure the continuity of existing payment gateways while demonstrating compliance with the PCI DSS standard through a comprehensive framework. Additionally, the architecture supports new evolving commerce protocols and, therefore, will work with generative AI platforms (e.g., ChatGPT and Gemini) while providing verifiable, immutable, and intended transactional action integrity to prevent the initiation of any unauthorised payments. The results of the implementation/evaluation of these components confirm increases in integration speed and payment transaction success rates compared to earlier methodologies. The proposed architecture reinforces the positioning of the capabilities required for conversational payments as a core competency, rather than a transactional extension from a web portal checkout. The future developments for the architecture will include enhancements related to voice-initiated commerce (i.e., via Amazon Alexa), decentralised payment methods, and improved mechanisms for identifying and dealing with fraudulent activities, thereby providing assurance for retailers to increase their confidence and success in the evolving marketplace associated with conversational commerce.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 1, January –February 2023||

DOI:10.15662/IJRPETM.2023.0601012

## REFERENCES

1. Authvia. (2021), "Trendy vs. Long Term Trends: Why Social Commerce is Here to Stay", https://www.authvia.com/blog/trendy-vs-long-term-trends/.
2. Authvia. (2021), "Authvia Appoints Three Industry Veterans to Its Board of Directors", Business Wire, https://www.businesswire.com/news/home/20210323005769/en/ Authvia-Appoints-Three-Industry-Veterans-to-Its-Board-of-Directors.
3. Cashfree. (2022), "Cashfree Payments – Year in Review 2021", https://www.cashfree.com/blog/cashfree-payments-year-in-review-2021/.
4. Eckoh. (2021), "Unaudited Interim Results for the Six Months Ended 30 September 2021", Eckoh Corporate Results, https://www.eckoh.com/news-insights/unaudited-interim-results-for-the-six-months-ended-30-september-2021.
5. Stream. (2021). The Top 3 Requirements for Developing a PCI DSS Compliant Chat App., https://getstream.io/blog/pci-compliant-chat-app/.
6. Cashfree. (2021), "Cashfree ties up with Aramex, goes global with payouts solution", ET BFSI, https://bfsi.economictimes.indiatimes.com/news/banking/cashfree-ties-up-with-aramex-goes-global-with-payouts-solution/80345365.
7. Eckoh. (2021), "Significant Cloud Contract Win", RNS Release / Shares Magazine, https://www.sharesmagazine.co.uk/news/market/LSE20211109070002_4171422/significant-cloud-contract-win.
8. US Patent No. 9,639,828. (2017), "Systems and Methods for Enabling Hosted Order Pages and Silent Order Posts to Reduce PCI Compliance Burden", https://patents.google.com/patent/US9639828B2/en.
9. US Patent No. 9,639,828. (2017). Hosted Order Page System and Method for Fraud Detection, https://patents.google.com/patent/US9639828B2/en.
10. Cashfree. (2021). Cashfree, PayPal to help Indian firms sell to 350 million customers. Business Standard, https://www.business-standard.com/amp/article/companies/ cashfree-paypal-to-help-indian-firms-sell-to-350-million-customers-121030200509 _1.html.