



---

A US PAYMENTS FORUM WHITE PAPER

# Emerging Payments Glossary

Version 2.0

October 2026

**U.S. Payments Forum**

544 Hillside Road  
Redwood City, CA 94062

[www.uspaymentsforum.org](http://www.uspaymentsforum.org)

## About the U.S. Payments Forum

The [U.S. Payments Forum](#) is a cross-industry body that brings stakeholders together on neutral ground to enable efficient, timely and effective implementation of emerging and existing payment technologies. This is achieved through education, guidance and alternative paths to adoption. The Forum is the only non-profit organization whose membership includes the whole payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on and have a voice in the future of the U.S. payments industry. The organization operates within the [Secure Technology Alliance](#), an association that encompasses all aspects of secure digital technologies.

EMV® is a registered trademark of EMVCo, LLC in the United States and other countries around the world.

All trademarks appearing in this white paper are the property of their respective owners.

## U.S. Payments Forum Emerging Payments Glossary

The U.S. Payments Forum Emerging Payments Glossary is an updated resource that defines a set of terms and standards that are commonly used and support clear understanding of emerging payments across the industry. Focused on terminology relevant to payment approaches, this resource was developed to garner cross-industry understanding of agent commerce and mobile and contactless payments terms and encourage the standardization of terminology.

The glossary is an updated collection of terms collected from existing U.S. Payments Forum payments glossaries as well as previously undefined terms provided by ecosystem stakeholders.

Where applicable, certain terms in this glossary are derived from or informed by concepts used in external standards, specifications, or industry frameworks (e.g., payment networks, ISO standards, EMVCo specifications). These definitions are provided for general informational purposes and may not be identical to, or a substitute for, definitions or requirements established in such external materials. Readers should refer to the relevant official documentation for authoritative definitions and requirements.

Additionally, certain terms relating to artificial intelligence, authentication, and emerging technologies are evolving and may be defined differently across implementations, vendors, or standards bodies.

Descriptions in this glossary are intended to be descriptive rather than prescriptive; they do not define required practices, assign responsibilities, or establish performance, security, or compliance expectations.

## Glossary

| Term                      | Updated Description                                                                                                                                                                                                                                                                                                                                          | Acronym/<br>Alias |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Abstract Consent          | A generalized authorization model in which a user grants permission for a class of actions or data access without specifying a single transaction instance, enabling systems or agents to operate within defined policy constraints until the consent is revoked or expires.                                                                                 |                   |
| Access Credential on File | Similar to Card on File, a payment arrangement in which an account owner authorizes a merchant or service provider to securely store a payment credential or token for a 3rd party digital account or digital wallet for simplified login authentication to be used in future transactions such as recurring payments, subscriptions, or expedited checkout. |                   |
| Agent Compromise          | A condition in which an unauthorized party gains control over an agent's credentials, execution environment, or logic, enabling fraudulent or unauthorized activity.                                                                                                                                                                                         |                   |
| Agent Credential          | A cryptographic or secret-based artifact (e.g., application programming interface [API] key, certificate, key pair, token) that an agent uses to prove its identity when accessing systems or initiating transactions.                                                                                                                                       |                   |
| Agent Endpoint            | The network or application interface (e.g., API endpoint, software development kit [SDK] interface, device channel) through which an agent exchanges messages or initiates commerce-related actions.                                                                                                                                                         |                   |
| Agent Identity            | The unique data and associated attributes that represent an agent within an ecosystem and are used for authentication, authorization, traceability, and audit.                                                                                                                                                                                               |                   |
| Agent Misbehavior         | Any deviation from authorized or expected agent behavior, whether accidental (e.g., bug, configuration error) or malicious (e.g., fraudulent or unauthorized actions).                                                                                                                                                                                       |                   |
| Agent Owner               | The entity that typically controls, secures, and configures an agent and may be responsible for aspects of its operation and use, depending on the applicable implementation, contractual arrangements, and governing frameworks                                                                                                                             |                   |
| Agent Registration        | The process by which an agent is created, verified, issued credentials, and assigned scoped permissions within a commerce ecosystem.                                                                                                                                                                                                                         |                   |
| Agent Stewardship         | The ongoing operational management activities that may be associated with an agent, such as monitoring, credential rotation, policy updates, performance oversight, and controlled decommissioning, depending on system design and governance models.                                                                                                        |                   |

| Term                              | Updated Description                                                                                                                                                                                                                                                                                     | Acronym/<br>Alias       |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Agent Verification                | The process of confirming the identity, credentials, and legitimacy of the user (i.e., individuals or entities) to help ensure compliance, security, and trust.                                                                                                                                         |                         |
| Agentic Commerce                  | A form of shopping in which an AI agent completes tasks for a user. The experience is facilitated via AI models – i.e., agents, which act as autonomous bots capable of setting goals, planning multi-step actions, and executing tasks across different environments with guidance from the user.      |                         |
| Agentic Commerce Transaction Type | The payment network classification for transaction types including: customer-initiated transaction (CIT); merchant-initiated transaction (MIT); agent-initiated transaction (AIT).                                                                                                                      | CIT<br>MIT<br>AIT       |
| Agentic Protocol                  | Technical framework designed to define how agents work with external tools, communicate their intent, set goals, or communicate with other agents to execute tasks. Examples may include: Modern Context Protocol (MCP), Agentic Commerce Protocol (ACP), and Agent2Agent Protocol (A2A), among others. | A2A<br>ACP<br>MCP       |
| Agentic Token                     | A secure, dynamic digital credential that allows AI agents to act on behalf of a human user within predefined, trusted boundaries. An agentic token encapsulates both user permission and specific transaction rules.                                                                                   |                         |
| Agent-Initiated Transaction       | Financial transactions executed autonomously by AI agents on behalf of a user without requiring human initiation.                                                                                                                                                                                       | AIT<br>Agentic Payments |
| AI Agent                          | Autonomous software systems powered by technologies like large language models (LLMs) and machine learning, designed to achieve specific goals with minimal human oversight.                                                                                                                            | AIA                     |
| AI Auditability                   | The capability of an AI system or process to be independently evaluated for compliance, safety, and fairness through thorough documentation, logs, and traceability of algorithms and data.                                                                                                             |                         |
| AI-Assisted Shopping              | The use of artificial intelligence such as chatbots, voice assistants, and recommendation engines to enhance and personalize the consumer retail experience.                                                                                                                                            |                         |
| Assisted Search                   | A search process that uses artificial intelligence or tools and allows users to enter queries in their own words to find an answer.                                                                                                                                                                     |                         |
| Attestation                       | A cryptographic process by which a device, application, or execution environment proves its authenticity and integrity to another system by presenting signed evidence about its hardware, software state, or security posture.                                                                         |                         |

| Term                            | Updated Description                                                                                                                                                                                                                                                               | Acronym/<br>Alias |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Avoidable Decline               | A legitimate payment transaction that is declined due to preventable issues rather than a legitimate business, risk, or fraud-related reason.                                                                                                                                     |                   |
| Authentication                  | The process of verifying that a user, device, or system entity is who it claims to be by validating one or more authentication factors such as passwords, cryptographic keys, biometrics, or possession-based tokens.                                                             | AuthN             |
| Autonomous Commerce             | An AI-driven system that independently manages the buying and selling of goods, automating complex, manual business-to-business (B2B) transactions and retail processes with minimal to no human intervention.                                                                    |                   |
| Autonomous Purchase             | A purchase in which a system or agent independently completes the transaction without human intervention at the moment of purchase.                                                                                                                                               |                   |
| Behavioral Monitoring           | A proactive technique used in cybersecurity to analyze, track, and record users and applications against an established baseline to identify anomalies, risks, or patterns of interest.                                                                                           |                   |
| Biometrics                      | A method of verifying an individual's identity based on measurable physiological or behavioral characteristics such as fingerprints, facial features, voice patterns, or iris recognition.                                                                                        | Bauth             |
| Bluetooth                       | A wireless communication technology that enables devices to exchange data over short distances using radio waves in the 2.4 GHz Industrial Scientific Medical (ISM) band.                                                                                                         | BT                |
| Business Application Identifier | A numeric or alphanumeric identifier used within payment processing systems to identify a specific business application, transaction type, or service associated with a payment message, enabling routing, processing logic, and reporting within financial transaction networks. | BAI               |
| Card Not Present                | A payment transaction in which the physical payment card is not presented, typically occurring in e-commerce, mail order, telephone order, or other remote payment environments.                                                                                                  | CNP               |
| Card on File                    | A payment arrangement in which a cardholder authorizes a merchant or service provider to securely store a payment card credential or token for use in future transactions such as recurring payments, subscriptions, or expedited checkout.                                       | CoF               |
| Card Present                    | A payment transaction in which the physical payment card is physically or digitally presented, typically occurring in retail and multilane environments.                                                                                                                          | CP                |

| Term                                           | Updated Description                                                                                                                                                                                                                                                           | Acronym/<br>Alias                                                               |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Closed Loop Mobile Payment                     | A mobile payment system in which the payment credentials, payment processing infrastructure, and acceptance environment are operated within a single organization's ecosystem.                                                                                                | Closed Loop                                                                     |
| Cloud                                          | A method for delivering computing resources that enables payment systems, data, and applications to scale on demand, improve resilience, and operate without reliance on on-premise infrastructure.                                                                           |                                                                                 |
| Cloud Wallet                                   | A digital wallet implementation in which payment credentials, tokens, and wallet-related data are stored and managed in cloud-based infrastructure rather than locally on a device, enabling access to payment functionality across multiple devices and channels.            | Wallet                                                                          |
| Consent Expiration                             | The predefined point in time or condition at which a previously granted user authorization becomes invalid, requiring renewed consent before further actions, transactions, or data access can occur.                                                                         |                                                                                 |
| Consent Mode                                   | The degree of authority that the consumer grants to the AI agent including when the intent was expressed and how long it is good for.                                                                                                                                         |                                                                                 |
| Consent Persistence                            | The capability of a system to retain and maintain a user's previously granted consent across sessions or transactions until the consent expires, is revoked, or is otherwise invalidated according to defined policies.                                                       |                                                                                 |
| Consumer Device Cardholder Verification Method | A method used during contactless transactions where a user verifies their identity directly on their own device – such as a smart phone or watch – using biometrics or a device passcode. Also known as “On Device Cardholder Verification Method.”                           | CDCVM<br>ODCVM                                                                  |
| Contactless Chip Card                          | A card containing an embedded microprocessor chip and contactless communication capability that enables transactions through short-range radio-frequency communication with compatible readers.                                                                               | CTL ICC<br>CTLS                                                                 |
| Contactless Payments                           | Any transaction method where payment credentials are transmitted wirelessly between a payment device and a contactless reader using Near Field Communication (NFC) protocols, typically completed by tapping or bringing the device within a few centimeters of the terminal. | CL Payments<br>MSD<br>CTLS Payments<br>EMV<br>Contactless<br>EMV CTLS<br>EMV CL |

| Term                            | Updated Description                                                                                                                                                                                                                                                                                                                                               | Acronym/<br>Alias                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Contactless POS Terminal/Reader | A point-of-sale reader equipped with contactless capability that can detect and communicate with contactless cards, mobile wallets, or wearables to process payments.                                                                                                                                                                                             |                                               |
| Coordinated Agent Attacks       | Threats which involve multiple autonomous AI agents working together to disrupt systems, perform malicious activities, or manipulate collective decision-making, often without direct, real-time human direction.                                                                                                                                                 |                                               |
| Credential Scope Creep          | The phenomenon where access permissions, API keys, service account privileges, or authentication tokens – initially granted with narrow, temporary, or limited scopes – may expand over time to become more than originally intended or authorized.                                                                                                               |                                               |
| Credentials Provider            | A software component, service, or system mechanism that manages, validates, and supplies user authentication credentials (e.g., username/password, keys, tokens) to securely access applications, systems, or services.                                                                                                                                           | CSP                                           |
| Customer-Initiated Transaction  | A transaction initiated directly by the cardholder through an interaction with the merchant or payment interface, where the cardholder actively participates in the payment authorization process at the time the transaction is performed.                                                                                                                       | CIT<br>Cardholder<br>Initiated<br>Transaction |
| Data Custody                    | The technical stewardship, guardianship, and protection of data throughout its lifecycle, including storage, transport, and usage, to help ensure integrity and security.                                                                                                                                                                                         |                                               |
| Data Encryption                 | The process of converting plaintext data into ciphertext using a cryptographic algorithm and encryption key so that the information is unreadable to unauthorized parties. Cryptographic algorithms include the Data Encryption Standard (DES), Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and Rivest-Shamir-Adleman (RSA) algorithm. |                                               |
| Delegated Authority Abuse       | The exploitation or overextension of delegated permissions by an agent to perform actions beyond the scope, frequency, value, or intent originally authorized by the principal.                                                                                                                                                                                   |                                               |
| Digital Payment Credential      | Secure, encrypted digital representations of physical payment cards or bank account details stored in digital wallets on personal devices.                                                                                                                                                                                                                        | DPC                                           |
| Digital Primary Account Number  | A tokenized version of a primary account number (PAN), typically assigned by a token requestor and loaded to a digital wallet.                                                                                                                                                                                                                                    | DPAN                                          |

| Term                                 | Updated Description                                                                                                                                                                                                                                                                                                                                                              | Acronym/<br>Alias         |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| Digital Wallet                       | A software application or service that securely stores payment credentials, tokens, and related payment information and enables users to initiate electronic payments through mobile devices, computers, or other connected devices.                                                                                                                                             | ewallet                   |
| Dual-Interface Card                  | A payment card that supports both contact chip transactions and contactless transactions by incorporating an EMV chip and a contactless communication interface.                                                                                                                                                                                                                 |                           |
| Dual-Interface POS Terminal          | A point-of-sale terminal capable of processing both contact chip transactions and contactless transactions, supporting communication with EMV chip cards through a physical card interface and with contactless cards or devices through radio-frequency communication. Note: "Hybrid" terminals accept contact and magnetic stripe cards only; they do not include contactless. |                           |
| Dynamic Card Verification Value/Code | A security feature where a three-digit CVV code changes periodically via a mobile app or a special display on a card. Used to combat fraud in card-not-present transactions.                                                                                                                                                                                                     | dCVV<br>dCVC<br>dCVx      |
| EMV 3-D Secure                       | An authentication protocol developed by EMVCo that enables issuers to verify cardholder identity during e-commerce transactions through risk-based authentication methods such as biometrics, one-time passcodes, or app-based confirmation before authorization is completed.                                                                                                   | 3DS<br>EMV 3DS            |
| Enrollment                           | The process by which a user, device, or payment credential is registered within a system, including the collection and verification of identifying information and the creation or provisioning of authentication factors or payment credentials.                                                                                                                                |                           |
| False Decline                        | The rejection of a legitimate payment transaction that should have been approved because fraud prevention controls, authorization rules, data limitations, or operational issues incorrectly identify a valid transaction as suspicious or unauthorized.                                                                                                                         | False Positive            |
| Federated Learning                   | A decentralized machine learning approach that trains AI models on local edge devices (like smartphones or servers) without sharing private, raw data.                                                                                                                                                                                                                           | FL                        |
| Fine-Grained Consent                 | A security approach that grants precise, granular access to specific resources, data, or actions rather than broad, "all-or-nothing" permissions.                                                                                                                                                                                                                                | Instruction-Level Consent |
| Funding Primary Account Number       | An original primary account number that represents the funding source of a DPAN.                                                                                                                                                                                                                                                                                                 | FPAN                      |

| Term                                                 | Updated Description                                                                                                                                                                                                                                                         | Acronym/<br>Alias |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Geofence                                             | A virtual geographic boundary defined using location technologies such as GPS, cellular, or Wi-Fi signals that enables systems to trigger actions, enforce policies, or monitor activity when a device enters, exits, or operates within the defined area.                  |                   |
| Geolocation                                          | The process of identifying or estimating the physical geographic location of a device using technologies such as GPS, IP address mapping, cellular triangulation, or wireless network signals.                                                                              | Geo               |
| Global System for Mobile Communications              | A digital cellular network standard adopted globally for mobile voice and data communications, forming the foundation for many mobile network technologies.                                                                                                                 | GSM               |
| Granular Consent                                     | The practice of allowing users to provide specific and detailed permission for different types of data usage rather than a single, all-or-nothing agreement.                                                                                                                |                   |
| Host Card Emulation                                  | A mobile technology that allows a device's operating system to emulate a contactless smart card and present payment credentials to a terminal without requiring a hardware secure element.                                                                                  | HCE               |
| Human in the Loop                                    | A governance pattern in which automated or agent-driven actions require human review, approval, or override under defined risk conditions before execution.                                                                                                                 | HIL<br>HITL       |
| Hybrid Terminals                                     | Terminals that accept magnetic-stripe (swipe) and contact EMV chip (dip) cards as opposed to dual-interface terminals which accept contact and contactless EMV chip cards in addition to traditional magnetic-stripe.                                                       | Hybrid POS        |
| In-App Payment                                       | A payment transaction initiated and completed within a mobile or software application where payment credentials stored in a wallet or payment service are used to authorize the purchase without leaving the application environment.                                       | In-App            |
| Indirect Prompt Injection                            | A security vulnerability where an attacker embeds malicious instructions into external data – such as websites, documents, or emails – that an LLM subsequently processes. The malicious commands are generally hidden in content the AI is designed to trust or summarize. |                   |
| International Organization for Standardization (ISO) | An international standards organization that promotes standards across multiple industries. ISO manages standards such as ISO/IEC 12812, ISO/IEC 12812, ISO/IEC 18092, ISO/IEC 14443, ISO/IEC 15420, ISO/IEC 19794, and the ISO/IEC 18000 series.                           | ISO               |

| Term                           | Updated Description                                                                                                                                                                                                                                                     | Acronym/<br>Alias                |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Know Your Agent                | A governance and due diligence framework for validating the identity, ownership, operational integrity, and risk posture of software agents before granting payment or token access privileges.                                                                         | KYA                              |
| Know Your Customer             | A governance and due diligence framework for validating the identity, data ownership, operational integrity, and risk posture of an entity's customer.                                                                                                                  | KYC                              |
| Limited Use Payment Credential | A payment credential designed for limited usage conditions, such as a single transaction, limited time period, or specific merchant or transaction type, to reduce fraud risk and restrict credential reuse.                                                            | LUPC<br>Limited Use Token        |
| Loyalty Front-End Processor    | A system that interfaces between merchant systems and loyalty program platforms to process loyalty transactions such as point accrual, redemption, and account updates during customer purchases.                                                                       | LFEP<br>Loyalty Host             |
| Magnetic Secure Transmission   | A contactless payment technology that allows mobile devices to emulate a physical credit card swipe at standard magnetic-stripe card readers.                                                                                                                           | MST                              |
| Merchant-Initiated Transaction | A payment transaction initiated by a merchant without direct cardholder interaction at the time of the transaction, pursuant to a prior agreement or authorization provided by the cardholder, commonly used for recurring payments, subscriptions, or delayed charges. | MIT                              |
| Mobile Check-In                | An application feature that allows users to indicate their presence at a physical location using a mobile device, often enabling personalized services, offers, or loyalty program interactions based on the user's location.                                           |                                  |
| Mobile Coupons                 | Electronic vouchers or discount codes delivered directly to a consumer's mobile devices that provide discounts, incentives, or promotional offers to consumers for products or services.                                                                                | Mobile Offers<br>Digital Coupons |
| Mobile Driver's License        | A digital alternative to a physical driver's license that contains all the necessary elements needed to validate the mDL holder.                                                                                                                                        | mDL                              |
| Mobile Loyalty                 | A system that enables consumers to earn, track, and redeem loyalty rewards through a mobile device or application as part of a merchant or brand loyalty program.                                                                                                       |                                  |
| Mobile Marketing               | The practice of delivering marketing messages, promotions, or advertisements to consumers through mobile devices using channels such as SMS, mobile applications, push notifications, or location-based services.                                                       |                                  |

| Term                                | Updated Description                                                                                                                                                                                                                                                                                                | Acronym/<br>Alias                  |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| Mobile Network Operator             | A company that owns or operates the infrastructure required to deliver wireless voice and data services to mobile subscribers under regulatory licenses.                                                                                                                                                           | MNO                                |
| Mobile Payment Application          | A software application installed on a mobile device that enables users to initiate, authorize, and manage payment transactions using stored payment credentials, tokens, or linked financial accounts.                                                                                                             | MPA                                |
| Mobile Payment Device               | An electronic device, such as a smartphone, tablet, or wearable, capable of initiating or processing payment transactions.                                                                                                                                                                                         |                                    |
| Mobile Payment Provider             | A company or platform that facilitates digital transactions via mobile devices, acting as an intermediary between customers, merchants, and financial institutions.                                                                                                                                                | MPP                                |
| Mobile Payment Provider Application | A cloud-based application provided by the mobile payment processor responsible for interfacing between the token vault or token/trusted service provider, the mobile payment application, the site system, and the payment front-end processor in order to authorize transactions.                                 | MPPA                               |
| Mobile Point of Sale                | A payment acceptance solution that enables merchants to process transactions using a mobile device, often combined with a card reader or contactless capability, instead of a traditional fixed point-of-sale terminal.                                                                                            | mPOS                               |
| Mobile Proximity Payments           | Payment transactions conducted using a mobile device that communicates with a nearby payment acceptance device through short-range wireless technologies such as NFC or Bluetooth.                                                                                                                                 | Contactless Payments<br>Tap to Pay |
| Mobile Remote Payments              | Payment transactions initiated through a mobile device in which the consumer and merchant are not physically co-located, typically conducted through mobile applications, web interfaces, or in-app payment flows.                                                                                                 |                                    |
| Mobile Wallet                       | A digital, app-based version of a physical wallet stored on a smartphone or wearable device, allowing users to securely store payment information, loyalty cards, and IDs.                                                                                                                                         | ewallet<br>Digital Wallet          |
| Multi-Factor Authentication         | A security process requiring users to provide two or more verification factors to gain access to an account or application. Encompasses three factors: something you know (e.g., password, PIN), something you have (e.g., smart phone app, SMS one-time passcode [OTP]), and something you are (e.g., biometric). | MFA                                |
| Multi-Merchant Bundles              | A specialized e-commerce feature allowing sellers in a marketplace to combine products from different vendors into a single, cohesive, and often discounted, offering.                                                                                                                                             |                                    |

| Term                       | Updated Description                                                                                                                                                                                                                                                    | Acronym/<br>Alias             |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Multi-Merchant Purchase    | A transaction where a buyer checks out once from a single platform, such as a marketplace, and the transaction is automatically split with two or more separate sellers.                                                                                               |                               |
| Near Field Communication   | A short-range wireless communication technology operating at 13.56 MHz that enables devices to exchange small amounts of data within a few centimeters, commonly used to support contactless payment, device pairing, and identity transactions.                       | NFC                           |
| NFC-Enabled Mobile Device  | A smartphone, wearable, or other consumer device containing an NFC controller and antenna capable of performing contactless interactions such as payment, ticketing, or identity verification.                                                                         | NFC Device                    |
| One-Time Password/Passcode | A dynamically generated authentication code that is valid for only a single login session or transaction and is commonly used as a second factor in multi-factor authentication processes.                                                                             | OTP                           |
| Open Loop Mobile Payment   | A mobile payment system in which transactions are processed through widely accepted payment networks (such as card networks or bank payment systems), allowing consumers to use payment credentials issued by financial institutions at multiple, unrelated merchants. | OLMP<br>Open loop             |
| Optical Reader             | A device that uses light to capture and interpret machine-readable patterns such as barcodes, quick response (QR) codes, or other visual data representations.                                                                                                         | Barcode Scanner<br>2D scanner |
| Pass-Through Wallet        | A digital wallet that does not store or manage payment credentials directly but instead tokenizes and passes payment data from a payment network or issuer through the wallet interface to the merchant or payment processor.                                          |                               |
| Passkey                    | A phishing-resistant authentication credential based on public-key cryptography that allows users to sign in to apps and websites using device-level biometrics or a screen-lock PIN.                                                                                  |                               |
| Payment Account Reference  | An alphanumeric identifier that links a consumer's underlying card account to all its associated digital tokens and reissued cards.                                                                                                                                    | PAR                           |

| Term                        | Updated Description                                                                                                                                                                                                                                                                   | Acronym/<br>Alias                                                                                   |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Payment Front-End Processor | A system or service that interfaces between merchant systems or payment gateways and payment networks or issuers to perform functions such as transaction routing, authorization messaging, formatting, and communication with payment networks.                                      | PFEP<br>FEP<br>Acquirer<br>Acquiring Processor<br>Payment Host<br>Mobile Financial Service Provider |
| Payment Orchestration       | The centralization of payment gateways, processors, and acquirers into a single platform, using one API to manage the entire payment lifecycle. It optimizes transaction routing to reduce failed payments and costs, supporting multiple payment methods and regional needs.         |                                                                                                     |
| Payment Service Provider    | A third-party non-bank service provider that enables merchants to accept and process electronic payments – e.g., payment gateway connectivity, transaction authorization routing, settlement processing, fraud management, and integration with payment networks and acquiring banks. | PSP                                                                                                 |
| Payment Token               | A security technology that replaces sensitive card numbers (i.e., the primary account number) with unique, randomly generated alphanumeric identifiers during digital transactions                                                                                                    | Token                                                                                               |
| Point of Sale               | A hardware device or integrated system used by merchants to initiate and process payment transactions by capturing payment credentials from cards, mobile wallets, or other payment instruments and transmitting transaction data to payment processors for authorization.            | POS<br>Point of Interaction (POI)                                                                   |
| Policy Token                | A cryptographically signed object that acts as a signed, executable rule set to authenticate actions or control access to services                                                                                                                                                    |                                                                                                     |
| Prompt Injection Attack     | A security vulnerability where attackers feed malicious, deceptive input into an LLM to override original developer instructions.                                                                                                                                                     |                                                                                                     |
| Protocol Stacking           | The use of multiple agentic protocols in a single workflow.                                                                                                                                                                                                                           |                                                                                                     |
| Provisioning                | The secure process of delivering, installing, and activating payment credentials, tokens, or payment applications onto a consumer device, digital wallet, or secure element, typically involving authentication of the cardholder and issuer authorization.                           |                                                                                                     |

| Term                           | Updated Description                                                                                                                                                                                                                                                                                                     | Acronym/<br>Alias                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| Pull Payment                   | A payment transaction model in which the merchant or service provider initiates a request to withdraw funds from the payer's account or payment credential pursuant to prior authorization, as commonly used in card payments and direct debit systems.                                                                 |                                         |
| Push Payment                   | A payment transaction model in which the payer initiates the transfer of funds directly to a recipient account, typically through real-time or account-to-account payment systems where the payer authorizes and sends the funds.                                                                                       |                                         |
| Quick Response Code            | A matrix barcode that encodes information in a two-dimensional pattern of black and white squares, enabling rapid optical scanning for applications such as payments, authentication, and information exchange.                                                                                                         | QR<br>QRC                               |
| Radio-Frequency Identification | A wireless technology that uses electromagnetic fields to automatically identify and exchange data with tagged objects or devices through radio signals. Used for contactless cards and NFC-based payment interactions.                                                                                                 | RFID                                    |
| Real-Time Purchase             | A purchase transaction in which authorization, clearing, and funds confirmation occur immediately or near immediately through an instant authorization mechanism. Merchants receive payment confirmation without the traditional batch settlement delay associated with card or Automated Clearing House (ACH) systems. |                                         |
| Relying Party                  | An entity that relies on an external identity provider or authentication service to verify a user's identity and then accepts the resulting authentication assertion to grant access to services or authorize transactions.                                                                                             | RP                                      |
| Rule-Based Purchase            | The use of automated, pre-defined "if-then" logic to make buying decisions rather than relying on manual, day-to-day human intervention.                                                                                                                                                                                |                                         |
| Secure Element                 | A tamper-resistant hardware module embedded in a device, subscriber identity module (SIM), or dedicated chip and used to securely store payment credentials, cryptographic keys, and execute sensitive payment operations.                                                                                              | SE<br>Embedded<br>Secure Element<br>eSE |
| Secure Remote Commerce         | A framework that standardizes a secure, interoperable digital checkout experience for card-not-present transactions by enabling consumers to store and retrieve payment credentials through network-managed systems, as defined and operated by participating payment networks.                                         | SRC<br>Click to Pay                     |
| Session Consent                | A time-limited authorization permitting an agent to act within the scope of a single authenticated session, expiring automatically when the session terminates.                                                                                                                                                         |                                         |

| Term                                | Updated Description                                                                                                                                                                                                                                                            | Acronym/<br>Alias                                                             |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Shopping Agent                      | Autonomous or semi-autonomous AI digital assistants that act on behalf of consumers to research, compare, and purchase products.                                                                                                                                               |                                                                               |
| Short Message Service               | A telecommunications service that enables the transmission of text messaging between mobile devices commonly used to deliver one-time passcodes or transaction notifications.                                                                                                  | SMS<br>Text Message                                                           |
| Staged Digital Wallet               | A wallet implementation model in which payment credentials or wallet functionality are partially provisioned or prepared in advance but are not fully activated until additional steps such as user authentication, issuer approval, or credential verification are completed. | Staged Wallet                                                                 |
| Standing Consent                    | A pre-approved, ongoing authorization that allows specific actions or transactions to occur repeatedly without requiring new approval each time.                                                                                                                               |                                                                               |
| Standing Policy Mandate             | A continuing directive that remains in effect indefinitely or until specifically revoked, governing ongoing conduct.                                                                                                                                                           |                                                                               |
| Static Card Verification Value/Code | A three- or four-digit security code that remains the same until the card expires. Used in payment transactions to verify the authenticity of a card and reduce fraud risk.                                                                                                    | CID<br>CSC<br>CVN<br>CVV<br>CVV2<br>CVC2<br>CVV<br>CVC<br>CVx<br>iCVV<br>iCVC |
| Store and Forward                   | A transaction processing technique in which transaction data is captured and temporarily stored by a device or system when real-time network connectivity to the payment processor is unavailable and then transmitted later when connectivity is restored.                    | S&F<br>SAF<br>SNF<br>Delayed Auth                                             |
| Subscriber Identity Module          | A removable or embedded chip used in mobile devices that stores subscriber identity information, network authentication credentials, and security keys used by mobile network operators to identify and authenticate a device on cellular networks.                            | SIM<br>SIM Card<br>Subscriber Identification Module                           |
| Token                               | A non-sensitive, reversible surrogate value that represents a primary account number (PAN) within specific transaction contexts; tokens are mapped to the PAN in a secure token vault or service.                                                                              |                                                                               |

| Term                          | Updated Description                                                                                                                                                                                                                                                                                  | Acronym/<br>Alias          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Token Lifecycle Management    | The processes and controls used to manage payment tokens throughout their lifecycle, including provisioning, activation, updates, suspension, replacement, and deletion.                                                                                                                             |                            |
| Token Requestor               | An entity (e.g., merchant, wallet provider, gateway) authorized to request tokens from a token service provider (TSP) to replace sensitive cardholder data (e.g., the primary account number) for use in transaction flows.                                                                          | TR                         |
| Token Service Provider        | An entity (e.g., network, issuer, or third party) responsible for issuing, mapping, managing, and validating tokens, as well as enforcing token policies.                                                                                                                                            | TSP                        |
| Token Vault                   | A secure, access-controlled repository that stores the mapping between tokens and underlying PANs (or other sensitive data), typically isolated from transaction processing environments.                                                                                                            |                            |
| Tokenization                  | The process of replacing a sensitive payment credential (e.g., the PAN) with a non-sensitive surrogate value (token) such that the token has no exploitable value outside the system while preserving required format for processing.                                                                |                            |
| Transaction Labeling          | The process of organizing, identifying, and tagging financial transactions with metadata to provide context on spending, income, and behavior.                                                                                                                                                       | Transaction Categorization |
| Trusted Agent                 | An entity delegated to perform specific, high-stakes tasks – such as identity verification, security clearance, or administrative actions – on behalf of a parent organization or authority.                                                                                                         | TA                         |
| Trusted Agent Protocol        | A defined set of cryptographic, attestation, and authorization rules that governs how trusted agents authenticate and interact with payment or commerce services.                                                                                                                                    |                            |
| Trusted Execution Environment | A secure area within a device’s main processor designed to help ensure that sensitive code and data are isolated and protected from the main operating system, enabling trusted execution of security-critical operations such as credential handling, authentication, and cryptographic processing. | TEE                        |
| Trusted Service Manager       | A service provider that manages the secure distribution, provisioning, and lifecycle management of payment credentials and applications to secure elements in devices such as mobile phones, SIM cards, or wearables.                                                                                | TSM                        |
| User Agent                    | Software or device that represents a user and interacts with another system on their behalf                                                                                                                                                                                                          |                            |

| Term                                 | Updated Description                                                                                                                                                                                                                                                                 | Acronym/<br>Alias                     |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| Universal Subscriber Identity Module | An advanced, secure smart SIM designed for 3G, 4G LTE, and 5G networks, offering improved security and higher data capacities compared to traditional SIM cards.                                                                                                                    | USIM                                  |
| User-Initiated Purchase              | A transaction that occurs when the cardholder actively triggers a payment, such as entering card details, using a payment card, or confirming an order online. Requires the customer's presence or direct action during the payment flow.                                           | CIT<br>Customer-Initiated Transaction |
| Wallet Service Provider              | A company that offers digital, virtual, or mobile platforms enabling users to store, send, and receive electronic money, cryptocurrencies, or payment credentials.                                                                                                                  | WSP<br>Wallet Provider                |
| Wearable Device                      | An electronic device designed to be worn on the body (e.g., smartwatch, fitness band, ring) that may incorporate sensors, wireless connectivity, and secure credential storage to enable functions such as contactless payments, authentication, and digital identity interactions. |                                       |
| Wireless Application Protocol        | A technical standard that enables mobile devices to access internet content like emails and web pages.                                                                                                                                                                              | WAP<br>WAP2                           |

## Legal Notice

This document is provided solely as a convenience to readers as a high-level, informational glossary of selected terms relating to emerging payments concepts. It is intended to promote general understanding and discussion only. This document does not establish, and should not be interpreted as establishing, any standard, specification, requirement, guideline, or recommended practice for the design, development, implementation, marketing, or operation of any product, service, or system.

While efforts have been made to ensure the information in this document is accurate as of the date of publication, the content is provided on an "AS-IS" basis, is subject to change without notice, and does not constitute legal, business, technical, or compliance advice. The inclusion or description of any term, concept, role, or example does not allocate responsibility, define duties, or prescribe outcomes for any participant in the payments ecosystem, and should not be relied upon for such purposes. All warranties of any kind, whether express or implied, including without limitation warranties of accuracy, completeness, non-infringement, merchantability, or fitness for a particular purpose, are expressly disclaimed.

This document is the result of voluntary collaboration among industry participants. Participation in its development does not imply agreement on any commercial practice, product design, market position, or competitive behavior. Nothing in this document is intended to, and shall not be interpreted to, (i) restrict independent business decision-making by any participant, (ii) coordinate or influence pricing, output, product offerings, or competitive conduct, or (iii) facilitate any agreement or understanding among market participants regarding commercially sensitive matters. All participants and readers are expected to act independently and in compliance with applicable antitrust and competition laws.

References to third-party technologies, frameworks, protocols, trademarks, or service marks are for illustrative purposes only and do not imply endorsement, affiliation, or standardization. All such intellectual property remains the property of its respective owners.

Readers seeking guidance on specific legal, regulatory, technical, security, or business matters should consult their own advisors, relevant standards-setting organizations, payment networks, and applicable official specifications.