A US PAYMENTS FORUM WHITE PAPER

Contextual Payments Considering Artificial Intelligence, 5G, and Internet of Things

Version 1.0

August 2025

U.S. Payments Forum
544 Hillside Road
Redwood City, CA 94062

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.

Executive Summary

This white paper explores the transformative potential of contextual payments within the realms of artificial intelligence (AI), 5G wireless technology, and internet of things (IoT). Contextual payments enable the promise of seamless transactions embedded within everyday activities, leveraging advanced technologies to enhance user experience and operational efficiency. By integrating AI-driven decision-making, high-speed 5G connectivity, and IoT-enabled devices, contextual payments offer an opportunity for a potentially frictionless and secure payment process that aligns with consumer behavior and preferences. The paper describes use cases, including smart retail, autonomous vehicles, smart homes, and healthcare, illustrating how these technologies can revolutionize commerce. Also addressed are critical considerations such as security, consumer consent, and infrastructure requirements. The white paper goal is to provide a broad overview to help orient and assist stakeholders considering how to navigate the complexities and opportunities of this innovative payment ecosystem.

Table of Contents

1. What Are Contextual Commerce Payments?

Contextual commerce is type of eCommerce where customers can make a purchase within the "context" of an activity without being directed to place a payment explicitly. *Contextual payment*s are the payments that occur within this environment, seamlessly, without the customer needing to produce a payment instrument or engage in a separate payment action. No direct checkout interaction takes place between the customer and merchant at the time of payment. Rather, these payments happen in the background, initiated by payment processing logic that assesses the circumstances of the situation and the consumer's prior authorized consent to make such payments. Data derived from geolocation, computer vision, biometrics, sensors, and/or computer logic of any kind is used to determine when and how much to charge a customer, what merchant accounts to apply to the transaction, and which payment instrument to use.

Contextual payments are a subset of *embedded payments*. Embedded payments involve integrating payment capabilities directly into an app or website without needing to switch to an external payment system. Both contextual and embedded payments aim to streamline the transaction process, but contextual payments emphasize the user experience, fitting naturally into what a consumer is doing at the moment. This makes them a more user-centric subset of embedded payments.

A well-known example of contextual payments is walk-out technology in retail locations. This technology uses a combination of sensors, computer vision, and artificial intelligence to track the items a consumer takes from the shelves. When the consumer leaves the store, the system automatically charges a pre-enrolled payment method. The payment is made automatically based on the "context" of actions within the store.

Another example of contextual payments is a smart refrigerator that detects when certain groceries are running low and automatically reorders them. The customer pre-enrolled a payment instrument, so they do not need to manually enter or select a payment instrument to complete a transaction. Instead, the smart refrigerator executes logic to place an order that is aligned to the customer's embedded preferences.

In both cases, payment occurs in the background and the customer has pre-approved the payment without using their physical card. Contextual payments leverage stored credentials with merchants or in-app purchases (where the consumer already stored their payment credentials). Using previously stored credentials ensures a seamless and convenient transaction experience without the need for physical cards or direct interaction at the time of payment.

Contextual payments also offer smart, seamless, automated transactions that occur within an IoT environment based on the user's current activity such as location, time, user behavior, or device activity. IoT ecosystems include smart devices across a variety of use cases. An example use case is the smart home where an IoT smart refrigerator initiates a transaction based on contextual triggers (e.g., ordering groceries). The payment is routed from the smart home to the merchant to the processor and issuer for approval. Once approved, the groceries are ordered and delivered without user intervention.

Figure 1 illustrates the IoT payment flow from different IoT ecosystems.

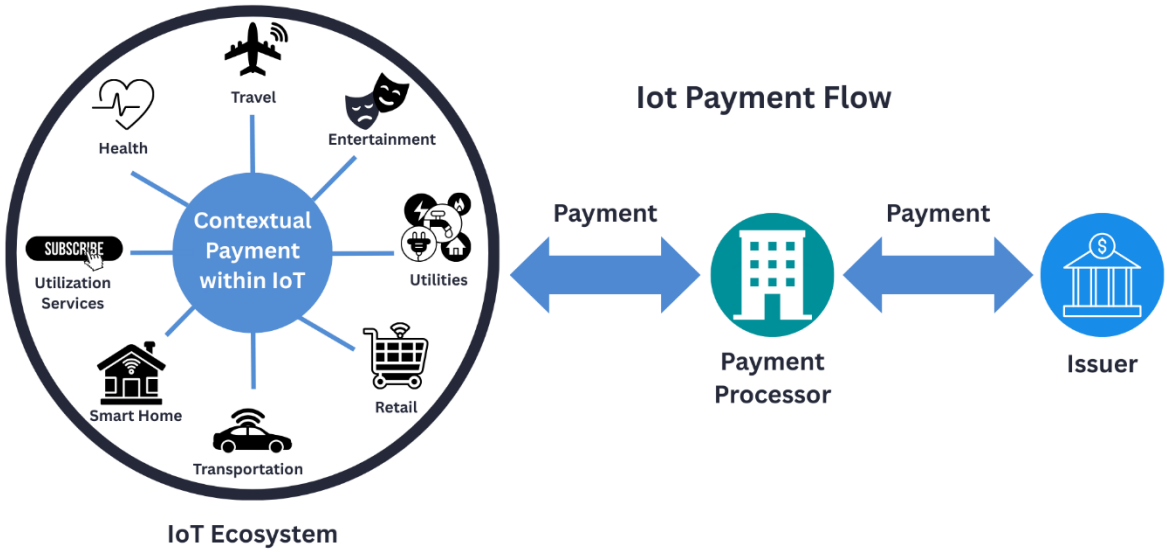

Figure 1. IoT Payment Flow

Agentic commerce is a type of contextual commerce where contextual payments can be made with even less interaction by enabling AI "agents." These agents can apply learned behavior preferences without requiring customers to take direct action during an activity.

An example of agentic commerce is travel booking. When a consumer is booking their flight, the agents have already been trained that the consumer has rewards at a certain hotel and prefers a specific rideshare company. The added intelligence can predict pick-up times needed for transport to the airport, book the hotel with the rewards points, and even ensure that the customer's coffee will be ready at a location they pass on the way to their gate. Implementing this added layer of intelligence has additional challenges that are discussed in Section 6.

Figure 2 illustrates the subsets of payments including embedded payments, contextual payments, and agentic commerce.

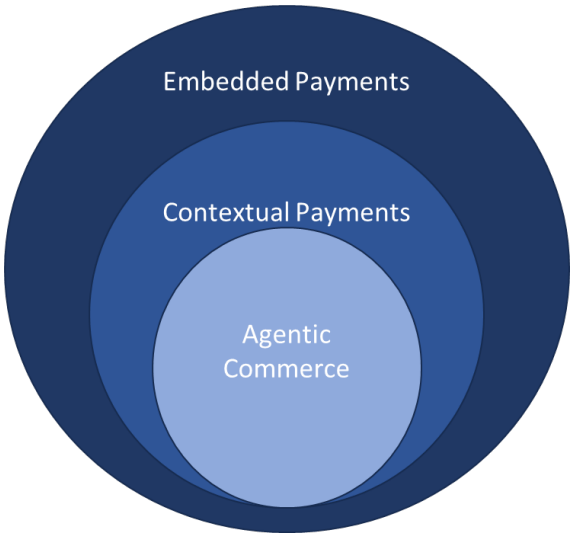

Figure 2. Subsets of Payments: Embedded, Contextual, Agentic Commerce

2. Intersection of AI, IoT-Enabled Devices, and 5G with Payments

2.1 IoT Relevance to the Emergence of Contextual Payments: Embedded AI in IoT

The growing role of AI has the potential to revolutionize IoT technology through automation and improved efficiencies. AI-powered IoT devices can gather, process, analyze, learn, and make smart decisions by accessing a massive scale of data. The proliferation of and ease of access to AI-powered IoT devices can in turn drive autonomous, seamless, and more secure contextual payments.

AI-powered IoT devices can learn user behavior, needs, and anticipated purchases and make autonomous payments through smart decisioning. The user experience can be improved by removing time-consuming, mundane, and repetitive friction. AI can provide recommendations based on customer preference so that merchants can offer more customized services while building loyalty.

Parking is an example of a commonly used service that can benefit from AI applying contextual payments without customer interaction. Customers can park and go by simply indicating the amount of time to be parked. An AI-enabled IoT device – such as a mobile phone, a radio frequency ID (RFID) device, or a smart vehicle – can complete the task of interacting with the parking system to share the vehicle license plate and parking zone number and complete a payment transaction seamlessly.

AI misuse tends to get more attention than its potential to protect. However, IoT devices with embedded AI may have applications that can make digital interactions safer for all participants in the contextual payment ecosystem. At the same time, AI can strengthen IoT device security through its intuitive fraud and scam protection for the customer, merchant, and processor.

2.2 5G Relevance to the Emergence of Contextual Payments: High-Speed IoT Connectivity

The global network infrastructure shift to fifth generation (5G) mobile communications has already transformed consumer and business experiences with improved communications, enhanced user experiences, and increased operational efficiencies. For consumers, 5G has introduced reliable high-speed connectivity to power IoT devices and new mobile applications ranging from connected vehicles, content streaming, to enhanced gaming.

High-speed communications can facilitate IoT-based vehicle technology using AI to access real-time data to help fleets optimize operational efficiencies. For example, access to real-time data allows IoT devices to optimize routing – for example, factoring in real-time variable toll costs, real-time traffic patterns, live vehicle fuel consumption, travel distance, parking location, and reservations – to direct the driver to the lowest priced fueling location based on the route and vehicle fuel levels. Contextual payment for all paid services can be initiated by the connected vehicle seamlessly without driver interaction or a physical payment instrument.

The advent of recent satellite direct-to-5G mobile phone connectivity can enable ubiquitous communications beyond the reach of existing terrestrial network coverage. High-speed communications can power IoT applications globally across broad sectors of commerce. Consumers will be able to initiate contextual payments globally simply by their presence. Businesses that operate fleets globally can centralize and streamline payment management through connected vehicles to facilitate cashless business-to-business transactions such as vehicle permits, tolls, parking, fuel, repairs, and maintenance. Layered with AI protection and decisioning capabilities, payments can transcend geographical boundaries that make commerce globally accessible and secure.

3. Contextual Payments Use Cases

Use cases for contextual payments exist in both business-to-consumer and business-to-business environments. This section discusses innovative examples of contextual payment in retail, transportation, smart homes, healthcare, entertainment, infrastructure, and business services.

3.1 Retail and Shopping

- **Smart retail and in-store payments**. Consumers can automatically pay for products as they walk through the store, with no need to stop at checkout counters. IoT sensors track items placed in carts, and payments are processed based on the items in the cart as the customer exits the store. This seamless experience eliminates the need for manual checkout processes, making the shopping experience faster and more convenient.
- **Voice-activated payments**. Payments can be made by simply speaking voice commands through devices like Amazon® Alexa® or Google Assistant™. For example, while shopping online, a user can simply say, “Pay for this item,” and the system will process the payment using voice recognition, linking to the user’s account or payment method.
- **Food delivery and take-out services**. Delivery platforms, such as food delivery apps, can automatically charge customers for food orders based on location, service charges, and consumption. The payment is processed when an order is placed or delivered, streamlining the food purchase process and making it more efficient for customers.
- **In-chat payments and conversational commerce**. Merchants are increasingly leveraging chat platforms not only to communicate with customers but also to facilitate purchases within the conversation. Secure payment links embedded in the chat or integrated payment functions within the platform can be used to perform the payment. For example, a customer might text their favorite restaurant to make a reservation. The restaurant can then offer a lunch special and process the payment, all within the same text message exchange. In-chat payment delivers a more personalized and immediate shopping experience, capitalizing on the customer's current intent and reducing the likelihood of cart abandonment.
- **Social media shopping**. Social media platforms are integrating "buy buttons," product tags with direct purchase options, and in-app checkout processes, enabling users to seamlessly purchase products they discover while browsing their feeds. A user scrolling through Instagram™ might see an advertisement for a piece of clothing they like and be able to purchase it with a single click without ever leaving the Instagram application. Social media shopping capitalizes on the discovery-to-purchase journey, turning social media engagement into direct sales opportunities by minimizing friction.

3.2 Mobility and Transportation

- **Autonomous vehicle payments**. Self-driving vehicles, equipped with IoT devices, can autonomously pay for services like fuel, tolls, or parking. The vehicle can communicate with payment systems and process transactions based on its journey, location, and service usage. For example, the vehicle might automatically pay for a toll when passing through a toll booth or for parking when parked at a meter.

- **Public transportation**. IoT-enabled public transportation systems can automatically charge users when they board or exit buses, trains, or subways. The system tracks the passenger's location or the fare zones traveled through and processes payment instantly without the need for manual ticketing.
- **Dynamic car rental payments**. Users renting vehicles can be charged based on the car's usage time, location, and additional services like GPS or insurance. Payments are automatically processed when the car is returned or when services are used, providing a smooth rental experience.
- **Smart parking and automated payments**. In cities equipped with smart parking systems, vehicles are automatically charged for parking as they enter and exit spaces. IoT sensors track parking time and payments are processed without requiring users to interact with parking meters or kiosks.
- **Contextual airport services payments**. Passengers at airports can automatically pay for services such as lounge access, priority boarding, or extra luggage fees based on their ticket type, usage, or location within the airport. These payments can be processed automatically through IoT integrations that track passenger movements and service interactions.
- **Connected car**: Information about connected car use cases is available in the U.S. Payments Forum's white paper, "Connected Car and Contextual Payments," available at: https://www.uspaymentsforum.org/connected-car-and-contextual-payments/.

3.3 Smart Homes and Healthcare

- **Smart homes and subscription-based services**. IoT devices within smart homes can automatically order and pay for items like groceries, toiletries, or cleaning supplies when stocks run low. Devices like refrigerators, washing machines, coffee machines, printers, or even smart speakers can monitor household consumption and ensure the house is always stocked with necessities.
- **Smart appliances and utility payments**. IoT-enabled appliances such as refrigerators, washing machines, or thermostats can monitor utility usage (e.g., electricity or water) and charge the user based on consumption. For example, a smart water meter could automatically bill a user based on the amount of water used in a particular period.
- **Wearables and health-related payments**. Wearable devices that monitor health metrics (such as fitness trackers or smartwatches) can track progress in wellness programs and automatically pay for services like health consultations, fitness programs, or supplements. Payments can be triggered when milestones are achieved or services are used.
- **Smart healthcare device payments**. IoT-enabled health devices, like glucose monitors or heart rate monitors, track a patient's health data and can automatically trigger payments for prescriptions, doctor visits, or therapy services when needed. These features could be helpful for chronic conditions, where continuous monitoring is required.
- **Instant product warranty activation and payment**. When a consumer purchases a product, an IoT-enabled system can automatically activate the warranty and charge for extended service plans or insurance. The system could use product data (such as purchase date or serial number) to trigger payment for additional protection plans or service packages.

3.4 Events, Entertainment, and Leisure

- **Smart events and ticketing systems**. Attendees at events such as concerts or conferences can automatically pay for additional services (e.g., VIP access, food, or merchandise) as they engage with various event features. IoT sensors in event venues can track attendance, movement, and service usage, allowing for seamless payment processing throughout the event.
- **Interactive museum and art gallery payments**. Museums or galleries can offer visitors interactive experiences using IoT-enabled devices, such as smart guides or augmented reality apps. Payments could automatically be made based on the content interacted with, such as special exhibits, interactive displays, or digital content accessed during the visit.
- **Contextual payments for streaming and digital content**. Users can be automatically charged for digital content like movies, books, or articles based on their interactions with the content. For example, when a user watches a certain amount of a movie or reads an article, the system processes the payment in real time for the consumed content.

3.5 Infrastructure and Utilities

- **Automated public utility management**. IoT devices in smart cities can monitor infrastructure like water pipes, electrical grids, or gas lines, detecting issues like leaks or surges. The system automatically processes payments for repairs, usage, or service fees based on real-time data.
- **Smart farming and agriculture payments**. IoT sensors on farms can monitor crop conditions, soil moisture, and environmental factors. When certain thresholds are met (e.g., low water levels or nutrient deficiencies), the system can automatically order agricultural supplies like water, fertilizers, or pesticides and process payment accordingly.
- **Smart public restroom payments**. Public restrooms equipped with IoT sensors can charge users for premium facilities (like showers, air dryers, or high-tech toilets) based on usage time. Payments can be triggered automatically when the user exits the restroom, offering convenience and reducing the need for manual transactions.

3.6 Business, Services, and Utilization-based Subscriptions

- **Contextual payments for shared office space**. Shared workspace platforms automatically charge for services like meeting room reservations, high-speed internet, or printing, based on usage. Payments are processed automatically when the service is used, streamlining the business operations of co-working spaces.
- **Contextual payments in the sharing economy**. Platforms like home-sharing services automatically process payments for services based on usage time, distance, or additional amenities. The system charges the user when the rental is completed, eliminating the need for manual transactions.

- **Contextual payments in digital news and magazines**. Consumers can be charged for individual articles, subscription content, or microtransactions based on their interaction with digital publications, simplifying the walled-garden or paywall model. This application creates a flexible payment model for non-subscription users while allowing media companies to capture revenue based on content engagement.

  (Note: Subscription services have added payment initiation complexity due to regulations.)

- **Dynamic pricing and real-time discounts**. Retailers or service providers can adjust prices dynamically based on demand, time, location, or customer behavior. IoT systems track when the customer engages with the service, and 5G technology facilitates the real-time processing of discounts, sales, and prices.

4. Benefits and Impact of Contextual Payments

Contextual payments can transform payments into a natural and intuitive process that benefits both consumers and merchants through convenience, personalization, efficiency, and greater security.

4.1 Consumers Benefits

- **Enhanced user experience**. AI-enabled IoT devices can automate and replace repetitive and time-consuming payments tasks through reduced friction. It can eliminate the need for manually entering payment information (which can introduce errors) or for navigating across separate payment apps. Transactions can occur quickly and smoothly within the user's current activity. For example, payment for a ride-sharing service occurs directly within the app or payment for parking can occur with the vehicle interacting with parking system to pay and extend parking sessions as needed. Users benefit from a frictionless checkout experience with contextual payments.
- **Increased access and Inclusivity** – Voice based and automated payments reduce the barrier for people with physical or cognitive limitations. Supports multilingual and localized content (currency).
- **Convenience**. Payment services can be integrated into apps and platforms for machine-to-machine interactions in common daily services. An example is a smart home where a connected heating, ventilating and air conditioning system and electric vehicle charger can operate at different times depending on the occupant’s presence or optimal utility rate. Utility bill payment is automated and completed effortlessly since use is optimized to achieve the greatest savings for the homeowner.
- **Intelligent payment routing**. Behind the scenes, contextual systems select the optimal card or payment method for each transaction. Consumers often are not even aware of which payment instrument was used—only that the system made the best choice.
- **Personalized experiences**. Consumers’ AI agents can interact with merchants by selectively communicating purchase history, preferences, and behavior to receive personalized offers and experiences. Consumers can benefit from time savings and convenience by purchasing relevant products or services and receiving personalized discount programs or loyalty rewards. For example, smart connected refrigerators can manage inventory, order, and pay for delivery from frequently shopped stores who offer tailored discounts based on purchasing history.
- **Payment security**. AI can introduce new levels of protection for the consumer by analyzing potential threats and adapting to evolving fraud tactics. IoT devices can interact with merchants to authenticate the consumer based on risk and purchase history. AI can evaluate the risks associated with the transactions. A newly registered or high-risk merchant may require additional security verification before a payment is released, thus protecting the consumer from potential scams. AI can manage and enhance payment through tokenization to protect account data from being compromised. In turn, these measures can benefit merchants by reducing or eliminating chargebacks.

4.2 Merchant Benefits

- **New customer experience opportunities**. Contextual payments open new opportunities for businesses to integrate personized services that could generate new revenue streams. Customized offerings can be delivered by enabling in-app IoT purchases or by providing flexible financing options based on a customer's line of credit or preferred payment methods. Businesses can offer personalized services that deepen customer relationships and grow loyalty through targeted and timely offers that resonate with the consumer's purchasing history and personal preferences.
- **Reduced checkout friction and cart abandonment.** Contextual payments can eliminate manual entry of payment information and drive transactions seamlessly and intuitively. Time savings and the ease of contextual payments can speed up online check out processes while lowering checkout abandonment.
- **Enhanced data insights and improved customer loyalty**. Businesses can leverage large amounts of disparate data from interconnected IoT devices to gain valuable insights into their customers' behavior, habits, and interests. This actionable information can be used to tailor marketing content, create personalized recommendations, and even target advertisements that meet customers' preferences.
- **Improved security and risk management**. AI can revolutionize payment risk decisioning by faster and more accurate analysis of a vast amount of transaction patterns and user behavior to detect and mitigate fraudulent activities. In turn, these measures can benefit merchants from reduced or eliminated chargebacks.

5. Shifting the Burden – From Consumer to Infrastructure

Contextual payments shift the burden of paying for products or services from the consumer to the back-end infrastructure. While this provides greater convenience and ease of use for the consumer, back-end systems must support new and complex features to support new functionality and deliver secure payments.

5.1 Back-End Complexity: What the System Must Manage

To deliver a seamless contextual payment experience, the underlying infrastructure must address complex, dynamic challenges, including the following:

- **Contextual decision engines**. Systems must analyze real-time data—such as location, time, merchant category, and past behavior—to determine whether and how a payment should be initiated. This function requires advanced AI and machine-learning models to optimize decisions like which payment method to use, whether to apply loyalty points, and when to defer or split payments.
- **Smart payment orchestration**. Payments may need to be routed across different payment rails—such as card networks, the Automated Clearing House (ACH) system, buy-now-pay-later (BNPL) providers, or the consumer's wallet balance—based on contextual rules. This orchestration also involves integrating with multiple issuers, wallets, and alternative payment providers in real time.
- **Real-time reward optimization**. The system must evaluate current promotions, merchant categories, and user preferences to apply the most beneficial rewards strategy. For example, it might select one payment method for grocery purchases and another for dining to maximize cashback or points.
- **Consent and control mechanisms**. Contextual payments require clear user permission across various devices and scenarios, including voice assistants, cars, appliances, and wearables. Systems must support granular controls, real-time alerts, and rollback options to maintain user trust and compliance.
- **Security and risk modeling**. Each transaction must undergo instant risk evaluation using contextual signals like device reputation, behavioral patterns, and environmental factors such as IP address and location. Based on these inputs, the system must decide whether to approve the transaction, escalate authentication, or block the transaction.
- **Data synchronization and identity resolution**. With payments originating from multiple touchpoints (e.g., smartwatches, apps, vehicles), maintaining a unified user identity and transaction history is critical. This demands robust identity graphing, tokenization strategies, and consistent data reconciliation across channels.

5.2 Areas of Impact

Table 1 summarizes the impact of contextual payments on consumers and infrastructure back-end systems.

Area	Consumer Experience	Infrastructure System Complexity
Checkout	No-touch, automatic	Context-aware triggers, real-time authentication
Payment Choice	Automatic use of the best payment vehicle	Rewards optimization, merchant mapping
Security	Low friction unless additional authentication is needed	Adaptive risk engines, device fingerprinting
Rewards	Automatic application or suggestion	Real-time rules engine for offers
Control	Easy overrides through an app	Permission management, audit trails
Privacy	Customizable preferences	Data minimization, regulatory compliance

Table 1. Impact of Contextual Payments on Consumers and Back-End Systems

Contextual payments shift the *burden of decision-making* from consumers to systems. This shift enhances usability—but only if the systems are built with robust logic, interoperability, security, and user trust at the core.

6. Considerations for Implementing AI-Driven Contextual Payments

This section highlights important considerations for implementing AI-driven contextual payments.

6.1 Consumer Consent

Consumer consent and data use transparency become critical factors for the success of any contextual or agentic purchase experience. In these scenarios, it is imperative that merchants or service providers are transparent in what data will be used and for what purpose. This transparency is especially true in the scenario where a customer may want to make a purchase that invokes a subscription or a merchant-initiated payment. Today, card-on-file merchant-initiated transactions are heavily regulated and require explicit consumer consent and prescribed notifications about pricing and timing of transactions. In the case of multi-party transactions, a method to notify customers that multiple transactions may appear on their statement is needed, but the process must be designed to not create friction that eliminates the benefits of frictionless ordering.

Classification of these types of transactions as customer initiated or merchant initiated will be a key deciding factor which rules apply.

6.2 Emphasis on Network Requirements

Contextual payment systems rely on real-time data processing, which requires high-speed network connections. These systems typically use wireless technology to perform their functions. Cellular networks (e.g., 5G, 4G) and Wi-Fi are examples of wireless technologies used. They provide broad connectivity options and enable devices to connect to networks or the internet wirelessly over large distances. These technologies are designed for high-speed data transmission, internet access, and interconnectivity between devices and networks.

Last-mile connectivity refers to the physical infrastructure and technologies between the internet service provider's network backbone and an end user, such as a merchant. This connectivity bridges the gap between the digital payment system and the point of sale or the recipient of the payment notification. Robust last-mile connectivity is important for enabling seamless and secure payment transactions in the physical world, particularly for use cases that require near-instant responsiveness between a merchant's physical location and the payment system, such as completing a purchase or receiving payment notifications.

A managed network service provider (MNSP) is typically employed to design, implement, monitor, and scale last-mile connectivity requirements. They can also establish redundancy measures to ensure backup connectivity and avoid service outages.

6.3 Security Considerations and Risk Factors

Security is a paramount concern with contextual payments and the subset of agentic commerce. Sensitive financial information and personal data must be protected from potential threats and unauthorized access. Establishing robust security measures can help to not only safeguard individuals' privacy but also maintain the trust essential for the widespread adoption of these technologies. Examples of security measures include the following:

Governance and Compliance

- Follow regulatory or compliance standards, including the Payment Card Industry Data Security Standard (PCI DSS), ISO 27001, ISO 15118, Security Operations Center (SOC), and privacy laws (including the California Consumer Privacy Act (CCPA) and other emerging privacy laws).
- For SOC, adhere to the five trust principles (availability, confidentiality, integrity, privacy, and security).
- Perform regular third-party audits, penetration tests, vulnerability assessments, and other tests and reviews for systems, personnel, and infrastructure.
- Establish data protection and security policies, procedures, and guidelines for employees, contractors, and other agents of the company, including privacy/security training, and system/data access rights with multifactor authentication (digital) or badge access (physical).
- Establish a cyber incident response plan, including the process and timeline for notices and applicable supervisory authority.
- Establish a disaster recovery and/or business continuity plan, including test plans.
- Establish secure coding practices (e.g., Open Worldwide Application Security Project [OWASP]) and web application security testing processes.

Data Access, Integration, and Storage

- For cloud-hosted systems and data storage, follow the Cloud Security Alliance standards.
- Encrypt data at rest using the AES-256 encryption standard and data in transit using TLS 1.2.
- Establish a data retention policy.
- Establish processes for account access, provisioning, and decommissioning, including third-party service providers and vendors.

Data Subject Rights

- Establish a data privacy notice policy that includes providing notices to consumers regarding collection, use, disclosure, and procedures to satisfy the data subject's right to access data. Define processes that manage requests in a timely manner.
- Establish procedures that satisfy data portability requests and deletion requests.
    - Implementers are advised to contact their security professionals to ensure that all applicable security, regulatory, and privacy standards are being followed.

Reliability

- Design and test the system to ensure reliable operation. For example, the system should prevent accidental orders – i.e., responding to the word "Alexa" in a television commercial.

Legal Considerations

All payments for services or goods are subject to applicable laws, regulations, and the terms of any associated legal agreements. For example, buying a plane ticket or movie ticket may require the customer to accept a specified refund policy. An agent may not be able to accept that agreement on behalf of the customer. Therefore, business legal departments need to be involved to enable agentic commerce and contextual payments.

6.4 Authentication

Authentication is the process of validating the identity of a registered user or process before enabling access to protected networks and systems. Authorization validates that an authenticated user or process has been granted permission to access the specific resource that has been requested. Identity management is the single most important component of any digital solution, and its operational and security integrity is critical. Authentication and identity management in the retail segment are generally tightly coupled to help minimize fraud and guarantee customer security. Identity management is the key operational and fraud control point; not having 100 percent visibility of the identity service can lead to outages, account takeover, costly fault-finding investigations, and latency in detecting and managing fraud. Careful consideration and implementation of the following will help support robust authorization and identity management in the contextual commerce environment:

- Authentication requirements for contextual commerce applications that include supporting and enabling marketplace applications, the underlying business relationships, and the user identity required to enable these partnerships.
- Authentication and identity management solutions that include multifactor authentication with consideration for PCI DSS, data protection regulations, and fraud prevention. Examples include using SMS as a second validation source, validating the mobile phone number/account, and using device-enabled biometrics.
- To support connected commerce applications enabled by third-party partnerships, authentication and identity management platforms that include support for different registration requirements, different verification/password reset standards and flows, different implementation of standards, and different security standards.
- An integrated approach to authentication, identity management, and security that is based on continuously predicting, detecting, learning, and protecting the user's identity in real time, making accurate decisions about new and emerging threats, and verifying authentic users. Related considerations include:
    - Device and user verification. Properly identifying the device and user to reduce the risk of spoofed identity or fraudulent purchases.
    - Card-not-present transaction best practices. Performing real-time verification that a card is linked to a valid account and repeating verification when each new transaction is performed.
    - Behavioral analytics. Continuously verifying the user is behaving as expected.

The broad success of contextual payments and agentic commerce will depend in part on the ability to bring integrated authentication solutions to the market that increase utility, while enabling digital collaboration, reducing customer friction, and supporting flexible solutions that overcome the following challenges:

- Varying registration requirements
- Varying verification/password reset standards
- Varying implementation of standards
- Varying interpretations of security standards

Additionally, strong industry collaboration may support implementation and the user experience, by helping to address the following complexities:

- Initial user onboarding complexities.
- Multiple logins and registrations to attach accounts.
- Decades-old consumer accounts with forgotten passwords and lost reset details. Data quality issues add to this complexity.
- Logouts that require the customer to re-login for each service.
- The need for customers to remember multiple passwords and account IDs.

As the number of devices and contextual commerce use cases rise, new identity use cases, innovations, and authentication methods will need to be considered to enhance the user experience without compromising security. Integrating everyday commerce into various environments through contextual triggers enables consumers to pay for goods and services, such as groceries, public transportation, online shopping, or anything else in a seamless and frictionless manner.

7. Enrollment and Provisioning

Enrolling a payment method into a contextual payment system is similar to the process used with other mobile wallets or applications that have payment capability. Service providers typically have an onboarding process for customers. The primary purpose of this process is to educate the customer and demonstrate key features and functionality. The onboarding procedure is responsible for helping the customer load and activate their payment credential in the system and companion smartphone application.

Alternatively, the consumer may need to use a display interface to add, update, or remove their payment credentials from the system if a device is being replaced, if the device is sold or damaged beyond repair, or if the consumer wants to add an alternate payment instrument. Depending on the system, enrollment and other changes could be done manually or via digital technologies, such as over-the-air Near Field Communication (NFC) provisioning.

As contextual payments are often designed to avoid the cardholder challenges of online authentication protocols (e.g., EMV 3D Secure), the importance of security during the provisioning process is increased. Friction can be minimized through a combination of provisioning with strong assurance (strong authentication), using payment tokens, including critical data (e.g., device information), and/or participating in a delegated authentication program.

8. Considerations for Stakeholders

Consumer Considerations

- **Control**. Transparency and direct consumer choice in selecting transaction participants will be critical to gaining adoption.
- **Cost**. Multi-party transactions could result in incremental costs as one merchant may take on the burden of the entire transaction and pass the resulting distribution fees to the other merchants and ultimately the consumer.
- **Consent**. Likely the most impactful consideration, customers will need to have clear paths to provide and revoke consent to perform transactions with their credentials. In the absence of strict guidelines meeting legal and regulatory requirements, consent implementation could also restrict the extent of use in recurring billing or subscription scenarios.

Merchant Considerations

- **Management and creation of consent mechanisms**. As consumer skepticism grows with automated processes or poorly executed AI experiences, consumer consent is critical to maintaining relationships with customers. Creating clean, informative, and transparent experiences will be key to ensuring the added simplicity does not come at the expense of consumer trust.
- **Data ownership.** Knowing your customer requires an understanding of customer preferences and preferred experiences with the merchant. The introduction of multiple parties or agents could shift data ownership to third parties and reduce merchant direct transparency.
- **Cost burden.**
    - Large-scale collaborative experiences introduce the concept of winners and losers in transaction economics. As new technologies emerge like blockchain or AI, transaction economics may become simpler, but today, many antiquated or expensive back-end processes are required for secure money movement between parties.
    - Emerging AI technologies (although potentially more efficient) may be costly. Early phases of implementation are focused on provider build-out vs. direct access for merchants. It will become more and more critical for merchants to have a voice in designing what solutions to leverage from providers and where it makes sense to create agentic experiences directly for their own customer base if they want to achieve truly customized (and affordable) solutions.

Processor Considerations

- **Latency and throughput**. 5G-enabled contextual payments will generate high-frequency microtransactions requiring near-instant processing.
- **Context-aware risk handling**. Processors will need to enable real-time decisioning engines using AI that factor in geolocation, device ID, merchant category, and other available information.

- **Standards and interoperability**. Application programming interfaces (APIs) and protocols for new contextual commerce environments (e.g., automotive wallets, smart vending) need to be defined.
- **Support for new form factors**. Payments will need to be enabled with consistent processing flows from many different IoT devices, including wearables, voice assistants, and more.

Issuer Considerations

- **Risk and fraud management**. Contextual payments will likely increase transaction volume and diversity, requiring enhanced fraud monitoring and addressing mechanisms. For example:
    - *Monitoring.* Issuers will likely need to enhance behavioral analytics, location-based verification, and device fingerprinting.
    - *Tokenization and data security*. Issuers may therefore need to prioritize the implementation of network tokenization to protect credentials that are embedded in IoT devices or wearables.
    - *Balance of risk and user friction.* Issuers may also need to use contextual risk signals to trigger additional verification only when necessary, minimizing fraud while preserving a smooth user experience.
- **Customer education and control**. Additionally, cardholders will may need management tools, such as dashboards to manage contextual payment authorizations (e.g., auto-pay from the refrigerator, car, or other device).
- **Interoperability and readiness**. Implementation should ensure compatibility with newer ecosystems (e.g., automotive wallets, smart home platforms).

9. Blockchain and Stablecoin

Many of the scenarios described in this white paper involve multiple merchant touchpoints in a single interaction. Today, legacy systems often require the following:

- Extensive verification of customer identity and risk assessments, also known as Know Your Customer (KYC).
- Dual vaulting, where the same customer data is stored and secured separately by the merchant and payment platform.
- Manual ledger reconciliation, which is the process of manually comparing and verifying financial records across different systems or accounts to identify discrepancies and correct them.

These siloed processes can often create unnecessary friction and inefficiencies. Traditional currencies are usually the primary use case for these scenarios; however, as stablecoin grows in popularity in U.S. markets, a future use case may use this currency or other popular cryptocurrencies for completing transactions. Stablecoins are digital currencies designed to maintain a consistent value, often by being backed and pegged to the U.S. Dollar or other real-world assets. Given this stability there is growing interest in how emerging technologies like blockchain paired with stablecoins could streamline interactions. Blockchain is a decentralized digital ledger that records transactions across a network of computers and ensures transparency and security by making the entries difficult to alter once confirmed. Together, stablecoin and blockchain could unlock a future where transactions happen automatically, at the right moment and in the right context.

Blockchain helps power this shift by acting as a secure, transparent digital ledger. When combined with smart contracts (essentially bits of code that say, “if X happens, then do Y”), payments can be triggered automatically when certain conditions are met. This combination removes many of the bottlenecks that can slow down traditional commerce like chasing invoices or waiting for manual approvals. Stablecoins extend this value by making the movement of money just as programmable and immediate. Stablecoins move quickly and can settle instantly, making them perfect for everyday payments. Since they work with the current payment ecosystem, businesses do not have to scrap their current system to move in this direction.

Both stablecoins and blockchain can work in the smart retail experience discussed in Section 3.1. In this retail use case, rather than stopping at a checkout line, customers simply walk out with their items. IoT sensors detect what has been taken, and a blockchain-based smart contract triggers an immediate payment in stablecoin to be quickly converted into U.S. Dollars. The transaction is secure, transparent, and logged into a single ledger – eliminating the need for manual reconciliation or redundant data storage.

Another example is the smart home use case, where a connected refrigerator detects low inventory and places an order automatically. Instead of generating an invoice, sending a reminder, and reconciling a charge potentially weeks later, a smart contract will start and settle the transaction instantly once the predefined conditions are met. Each step is traceable and secure.

Together, blockchain and stablecoin can enable a smarter, more responsive architecture for contextual payments. With close to real-time money exchanges and rules-based transactions, businesses can reduce overhead, improve liquidity, and operate more efficiently. For consumers, this translates into seamless payment experiences, whether they are shopping online, using a connected device, or interacting in entirely new digital environments. And for a larger ecosystem the combination will open the door to payments that are faster and more connected.

It should be noted that various payment rails will be powering contextual payments depending on the use case. As the current landscape heavily depends on card payments or bank accounts, payments may shift to stablecoins or other blockchain solutions. Customers who do not want to share their card or bank details with vendors may prefer to use wallets. These wallets in turn can be funded by cards, bank accounts, or cryptocurrency accounts. Stablecoin “machine-to-machine” payments have the potential to be faster with minimal reconciliation issues. Smart contracts can help to ensure that the delivery of services is aligned with the payment.

10. Conclusion

In conclusion, the combination of AI, 5G, and IoT in contextual commerce payments is set to transform the landscape of digital transactions across retail, housing, mobility, entertainment, and other sectors. Technology synergies will drive unparalleled levels of convenience and personalization in a secure way. Bringing this convenience to the consumer will shift transactional responsibilities from consumers to the infrastructure, requiring effective management of complex back-end systems to ensure seamless experiences. This white paper serves as a wide-ranging guide for helping stakeholders to better understand, prepare for, adopt, and leverage the transformative power of contextual payments and agentic commerce, highlighting stakeholder considerations such as infrastructure requirements, security, and authentication. Technological convergence offers vast opportunities for innovation in contextual payments.

11. Legal Notice

This document is provided solely as a convenience to its readers, as a high-level overview of contextual payments and associated considerations for payments stakeholders relating to artificial intelligence (AI), 5G wireless technology, and the internet of things (IoT). The particular considerations, costs, benefits, and technologies discussed in this paper do not represent an exhaustive list. Accordingly, considerations, costs, benefits and technologies that are not addressed in this paper may be as or more important to a given organization than those described herein when deciding how best to navigate the complexities and promise of contextual payments in the evolving payments landscape. While great effort has been made to ensure that the information provided in this document is accurate and current, this document is informational only, is not legally binding, does not constitute legal or technical advice, and should not be relied upon for any legal, technical, or other purpose. Accordingly, all warranties of any kind, whether express or implied, relating to this document, the information herein, or the use thereof are expressly disclaimed, including but not limited to warranties as to the accuracy, completeness or adequacy of such information, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. Any person that uses or otherwise relies on the information in this white paper does so at his or her sole risk. Without limiting the foregoing, it is important to note that this document provides only a high-level description of the subject matter; and the concepts described in this paper should not be considered standards, requirements, recommendations or guidelines. Readers interested in implementing or exploiting contextual payments, AI, 5G, or IoT as part of their payment processes should therefore consult with their respective security providers, subject matter experts and professional and legal advisors, as well as relevant payments industry stakeholders, such as payment networks, issuers, acquirers, and others, prior to any implementation decisions.