

INITIAL CONSIDERATIONS

Defining “Omni-Channel”

If we look at the prefix “omni”, it simply means “all”. Though impractical to accept all commerce mechanisms, the more commonly accepted definition is to accept the three primary types of electronic payment: in-person, in-app, and in-web. The core issue in accepting these is delivering a unified and consistent experience across the platforms. In the following, we discuss what needs to be considered when constructing an omni-commerce platform and review the advantages and disadvantages of each decision.

Initial Decisions

1. DO I WANT MY APPLICATIONS TO HAVE THEIR OWN EMVCO CERTIFICATION

While this is pertinent to in-person only, it is often overlooked.

PRO

Having one’s own certification allows developers to have the greatest flexibility with the in-person app narrative, branding, and access to data. Exploring this option may include manufacturing a custom hardware solution.

CON

While this may deliver the most customized experience and provide access to the most data, this option isn’t for everyone since it is a significant effort, sometimes spanning years, with great expense to build-out and certify.

Using third-party partnerships is more common and can be more advantageous since it can accelerate time-to-market and reduce initial overhead expenditure.

2. DO I WANT MY APPLICATIONS TO BE PCI-VALIDATED

This applies to each of the omni-commerce payment channels.

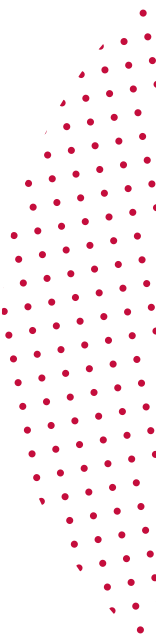
PRO

Accepting PCI requirements in an application allows for the best visibility to data. Data drives the customer experience, so it only makes sense that data has value.

CON

PCI validation is often viewed as a major undertaking, and assessing if the value meets or exceeds the requirements of PCI needs to be an individual determination.

Partnering with security-focused companies is the most common approach to meeting PCI requirements. This increases time-to-market and saves infrastructure efforts to secure data within applications.





Definitions for Each Channel

WHAT DOES “IN-PERSON” ENCOMPASS

In-person is the electronic exchange of commerce where the buyer has a physical payment instrument interact with a payment acceptance device. This could be a card-present credit card tap, dip, or swipe, mobile wallet like Apple® Pay or Google™ Pay, or an instrument used for stored value (bracelet, ring, etc.). This is presented in a multitude of environments including traditional countertop, mobile (line-busting, delivery, or pay-at-table), and kiosk.

WHAT IS “IN-APP”

In-app is simply a consumer driven payment that is executed on a native application loaded to a personal device. These are inherently card-not-present transactions. The consumer types in the payment information into a payment page on the application or uses a pre-constructed payment credential like a card saved on file, token, or QR code. It can also include paying by Apple Pay or Google SmartTap if this has been built into the payment application.

HOW IS “IN-WEB” DIFFERENT

Like in-app, in-web is a consumer driven transaction, but is not predicated on a native application being present on a personal device. This is often referred to as an eCommerce transaction. While the same payment flow occurs as in-app, the transaction happens on a page loaded in a web browser rather than an application downloaded locally.

SECONDARY CONSIDERATIONS

Combining All Three

To develop a genuinely omni-commerce experience, the user must have minimal conflict-of-use, recognize the user, and know their payment instruments across the channels. PCI scope reducing implementation and important services need to be considered when the full flow of payment data is not at the fingertips of the application.

3. HOW WILL YOU IDENTIFY CUSTOMERS

The easiest way to identify customers is to have them provide their consent and create a profile when engaging in one method of commerce and then share the information across the three commerce methods. Autofill-in web browsers and in-app capable of leveraging a browser makes this easy. Without identifying the customer, merchants are unable to track or engage with customers, limiting retargeting campaigns, and the value of the payment application.

4. WILL TOKENS BE USED FOR PAYMENT INSTRUMENTS

A payment instrument includes a physical item e.g. credit card, a digital item e.g. mobile wallet, or a digital “token” of payment data. Tokenized payment instruments are typically preferred since they do not require PCI validation. When considering a tokenization solution, it is beneficial to ensure the customer profile information works across merchant brands. For example, if Jenny’s Café uses the same application as Rob’s Bistro, two unaffiliated businesses, the customer profile information ideally would work as a consistent payment instrument. If it does not, it can cause aggravation to the customer and create unnecessary pain points.

5. HOW WILL YOU IDENTIFY PAYMENT INSTRUMENTS

Having identifying indicators becomes important to tie secure payment instruments to a consumer that cross all payment channels. Some payment instruments are form-and-format preserving, this makes them easy to identify and track from outside (potentially malicious) sources, heightening awareness of activity in those environments. Whereas, many tokenized payment instruments don’t have the look or feel of important data, making them easy to ignore, and more difficult to identify and match to a consumer.

6. WHAT WILL BE THE ACCEPTED PAYMENT TYPES

Lastly, it is important to meet the consumer where they are. Cash, card, check, Apple Pay, Google Pay, Venmo®, PayPal® are all considerations for a wide range of consumer identities. Being able to make the consumer comfortable in their experience means repeat usership. Though adding more payment types can increase the development effort, third-party partners ease this difficulty, and the benefit far outweighs the cost.

CONCLUSION

A systematic approach is necessary when developers implement an omni-commerce solution. Core business and application design decisions need to be thought-out across all platforms before beginning development in one platform. This saves on development effort, compliance and certification strategy, and determines the best partnerships to achieve business objectives.

MagTek and Magensa provide the essential building blocks, services, devices, knowledge, and guidance to help independent software vendors (ISVs) build robust omni-commerce solutions. Partner with us to streamline the development process and deliver a seamless, secure, and comprehensive omni-channel customer experience.

About MagTek

Founded in 1972, MagTek is a leading manufacturer of electronic systems for the reliable issuance, reading, transmission, and security of cards, barcodes, checks, PINs, and identification documents. Leading with innovation and engineering excellence, MagTek is known for quality and dependability. Our hardware products include secure card reader/authenticators, Quantum secure cards, token generators; EMV Contact Chip, EMV Contactless, barcode and NFC reading devices; encrypting check scanners, PIN pads, and credential personalization systems. These products all connect to Magensa, a MagTek owned gateway that offers businesses the ability to securely process transactions using authentication, encryption, tokenization, and non-static data.



MagTek is headquartered in Seal Beach, CA, please visit www.magtek.com to learn more or contact us at www.magtek.com/contactus.