A Guide for Mobile Product Managers

QR code contactless payments

Designing for security & convenience

INCOGNIA™

Introduction

QR codes have seen a surge of adoption in the US during 2020, as a convenient and easy to deploy method for contactless payments. This ebook is designed for product managers who are responsible for retail and loyalty mobile apps and looking to better understand the rising interest in QR Code contactless payments. In this eBook we will review how QR codes work and important security and convenience design features to consider when incorporating QR codes as a mobile payments feature.

Incognia
Palo Alto
November 2020

Why QR codes? Why now?

While contactless technology has been around for several years, adoption in the US has been slow until recently, with a surge in usage largely due to health concerns associated with the COVID-19 pandemic. With the recent introduction of QR code contactless payments by PayPal and Venmo, QR codes are enabling not only a contactless, but also a frictionless, form of payment. **Mastercard reported a 40% growth in contactless transactions worldwide in the first quarter of 2020** alone and 70% of people say they will switch to digital payments permanently. In addition to reducing the risk of infection, the main benefit of contactless payments to customers is the removal of friction. With touch-free technology, customers can use their mobile phones as wallets.

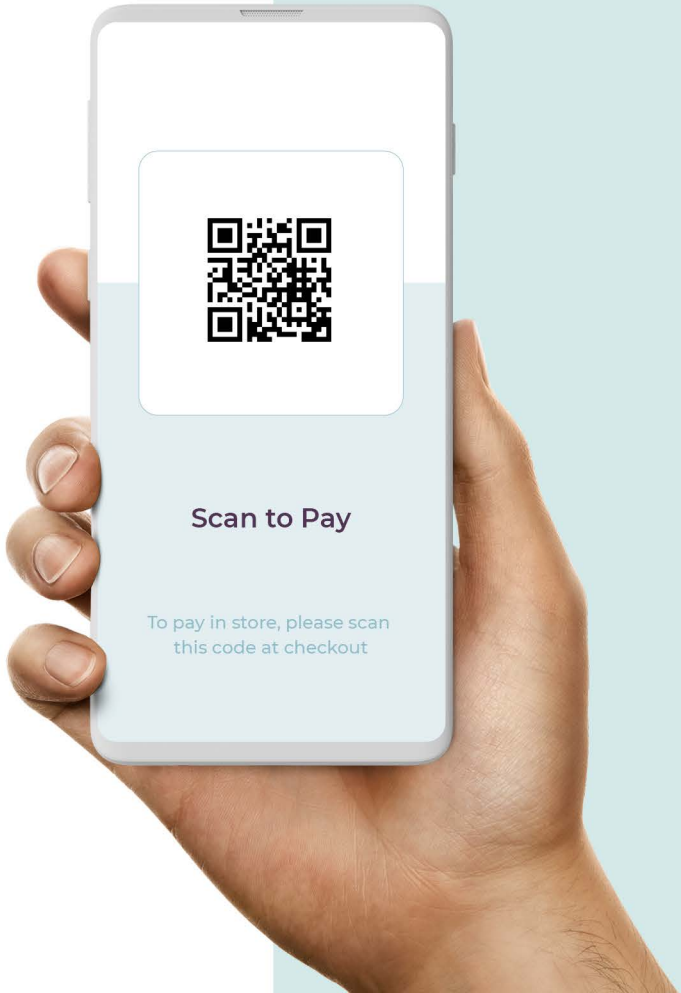
There are two distinct technologies that enable contactless payments solutions, **NFC** (Near Field Communication) and **QR** (Quick response) codes, and both utilize tokenization to turn data into a string of characters called a token.

NFC
Near field communication

QR
Quick response

40% growth in contactless transactions in Q1 2020

Source: Mastercard



Surge in interest in QR codes

The use of QR Codes for contactless payment has seen the biggest surge in usage. The advantage of QR codes over NFC technology is that **QR codes can be sent and received by any smartphone, requiring no point-of-sale (POS) infrastructure.**

With the disruption of social distancing, many retailers and restaurants are looking to rapidly upgrade their payment processes to support contactless payments. QR code technology makes it easy for merchants to either provide a QR code or scan a user's code, depending on process preference and data connectivity. For the merchant, this can eliminate the cost of a POS system and the fees associated with accepting credit cards. For the user, this means less friction and more convenience, leading to increased conversions for the merchant.

More convenience and ease of implementation led QR code payments to be rapidly adopted in China, resulting in the current payment ecosystem where cash and credit are rarely offered. Alibaba and Tencent are responsible for driving the shift away from cash, with Alipay and Wechat Pay apps accounting for 90 percent of the $17 trillion mobile payments market in 2017. Of this $5.5 trillion in 2016 was QR code mobile payments.

QR code contactless payments require no point-of-sale (POS) infrastructure.

QR Codes as a replacement to chip & PIN credit cards

Contactless mobile payments are a natural next step for users who are increasingly managing their finances through mobile apps, including banking, investing and applying for credit. The convenience and security of mobile payments is defining the speed of adoption. With the mobile phone acting as a payment vehicle, the traditional wallet can now stay at home. The days of forgetting your wallet are over.

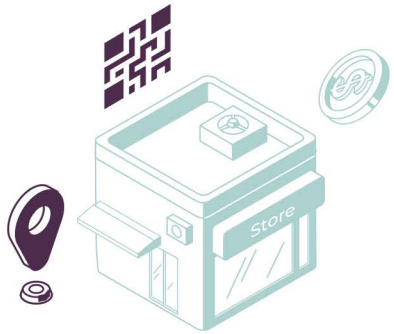
Use of QR code payments within mobile apps

With QR Code usage on the rise, merchants are leveraging their existing loyalty mobile apps to rapidly add contactless payment capabilities. For the user, this means that a merchant's mobile app can now become a virtual wallet, enabling contactless transactions.

Retailers, merchants, banks, fintech and payment providers are rushing to meet the demand. Recent high profile announcements include the roll out by Albertsons of contactless payment within its U loyalty app to enable streamlined checkout and payment at all their stores. Also, ExxonMobil recently announced that over 11,500 stations in the US would be upgraded enabling customers to pay for gas without needing to interact with staff.

Albertsons and Exxon Mobile are both examples of retailers moving quickly to include support for QR code contactless within their loyalty mobile apps, enabling customers to use their smartphones and scan a QR code to make a contactless payment.

It is not only in stores and at gas stations that consumers are opting for contactless payments. Diners in restaurants around the world have rapidly adopted contactless payment methods. Starbucks is no longer alone in enabling payments via its mobile app. Today both independent restaurants and chains are enabling diners to scan a QR code to pay their bills either via mobile apps or the web browser. Diners who have the app installed can scan the code and pay for their bill from the app, electing to add a tip if they choose to do so. Customers can add credit cards or bank details to the app, allowing them to pay with either.



QR code contactless payments

How it works

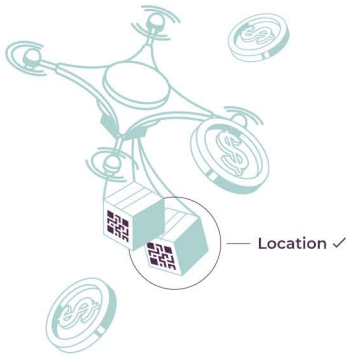
There are three key uses for contactless payments:

In store payments

A consumer has reached the check out and is ready to pay. With QR codes there are two options for payment, either the consumer scans the merchant's QR code, or the merchant scans the consumer's QR code.

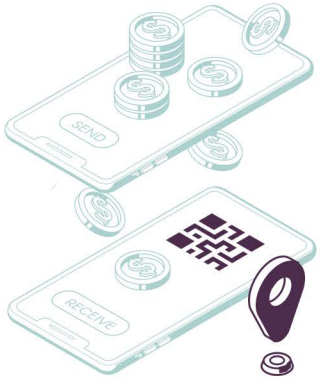
For example, a consumer is in a store that accepts PayPal QR code payments. The consumer has a PayPal account and a personal QR code which identifies the consumer's payment details. The merchant scans their code and the payment is confirmed.

In the alternate scenario, the consumer reaches the checkout and is presented with the merchant's QR code. In this case, the consumer receives a token from the merchant containing the amount, currency and store information. The payment provider, either the app itself in the case of AliPay or Visa or Mastercard, confirms the payment and sends a confirmation to the merchant and consumer.



Remote payments

A mobile shopper has reached the the checkout page for an ecommerce purchase and is ready to pay. The user selects QR contactless payment as the payment optionwith their mobile app. The user is shown the transaction amount and is instructed to scan the QR code to confirm the transaction.



Peer to Peer payments

User 1 wants to transfer funds or make a payment to User 2. User 1 presents User 2 with their personal QR code to confirm the payment. User 2 is shown the transaction amount and is instructed to scan the QR code of User 1 to confirm the transaction.

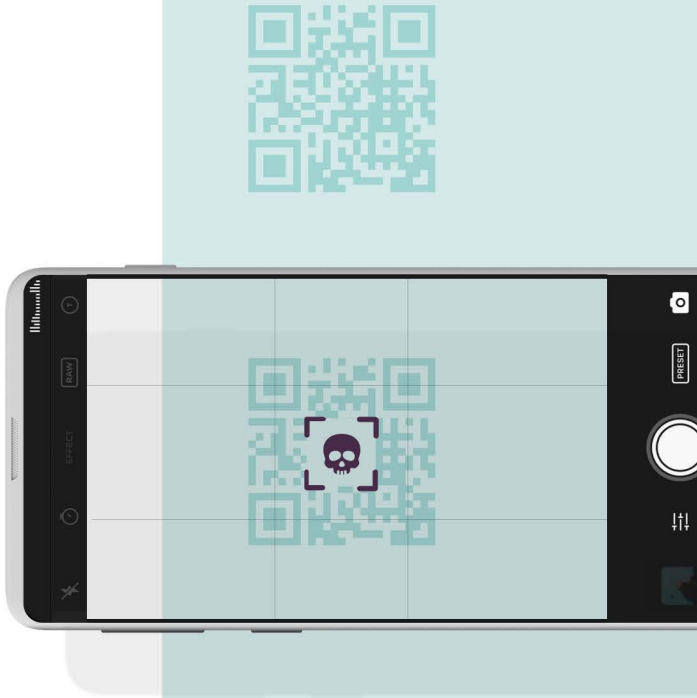
In each case, the user wants to make a payment either to a merchant or to another individual. In order to complete the payment, the user is presented with a QR code which they scan to exchange payment details.

Protecting against fraud

Like any digital payment solution, contactless payments are susceptible to fraud. Social engineering attacks, including phishing scams, are not only targeted at websites but also increasingly QR code payments. A malicious QR code can lead unsuspecting consumers to a form designed to steal credentials or personal information or to initiate a download of malware. Given that most payment-enabled QR codes are stored within apps, they are also at risk of account takeovers.

That said, the specific characteristics and use cases of QR codes has led fraudsters to implement new techniques. QR codes look the same to the naked eye whether they were generated to send or receive a payment. Given this, one of the biggest threats to QR users is unintended money transfers. Fraudsters might send a QR-code claiming that the recipient will receive money or benefits by scanning it when in fact it triggers an automatic transfer.

They can also be posted anywhere, both physical or digitally, and can be scanned by most smartphone models popular today. Fake QR codes can easily be staged to look legitimate, especially when printed, causing unsuspecting people to pay a fraudster rather than the person or merchant they intended. In China, a popular scam entailed placing fraudulent QR-enabled parking tickets on cars leading to the theft of thousands of dollars. For merchants, this could mean lost revenue and chargeback fees.



3 Important design considerations for security & convenience

Given the use of QR code contactless payments is new for many merchants and users in the US, there are three important design considerations to ensure a safe and frictionless experience for the user.

01

Onboarding

Many users are new to QR Code contactless payment. This means that many will open new accounts while in the store and at the exact moment of purchase leaving little room for time-consuming new account application processes that could jeopardize conversions. Merchants need to make sure that they provide a frictionless, speedy experience for identity verification at onboarding to increase adoption of this new payment method.

02

Login

QR codes, like other in-app payments, are susceptible to account takeover attempts. In fact, given the novelty of this payment method, users may be particularly vulnerable. Authentication of QR code contactless payments should ensure that the user requesting the transaction is in the location of the store.

03

Payment

Fake QR codes are a real thing. They can easily be staged to look legitimate, especially when printed, causing unsuspecting people to pay a fraudster rather than the intended person or merchant. Additionally, illegitimate QR codes can result in automatic downloads of malware. Mobile apps should incorporate fraud detection checks to ensure that the QR code being scanned is associated with the merchant location, and that the customer is at the location of payment.

Meet Incognia

Fraud detection for QR code contactless payments

Incognia's frictionless QR code fraud detection solution works behind the scenes to authenticate in-store, remote and P2P QR payments. Incognia helps companies prevent the most commonly known attacks in QR code payments: account takeovers, fake accounts and fake QR codes.

Through location behavioral biometrics, Incognia creates a private digital identity for each user (like a location fingerprint), turning the smartphone into a dynamic token. This location-based risk assessment enables companies to authenticate remote and in-store mobile transactions to prevent account takeover and payments fraud. By checking the user's real-time location, Incognia can determine whether, in real-time, whether the user is transacting from a trusted location or a legitimate point-of-sale, based on their historical behavior, and if the scanned QR code is associated with that specific merchant.

Incognia is implemented as an SDK within both iOS and Android Mobile Apps and protects the user throughout their experience, from initial onboarding to authentication and contactless payment transaction. The Incognia SDK collects device and location data and via APIs returns a risk assessment based on user location behavior.

Frictionless onboarding verification

Incognia uses location intelligence to match the home address provided during onboarding to the user's real world location behavior.

Secure login authentication

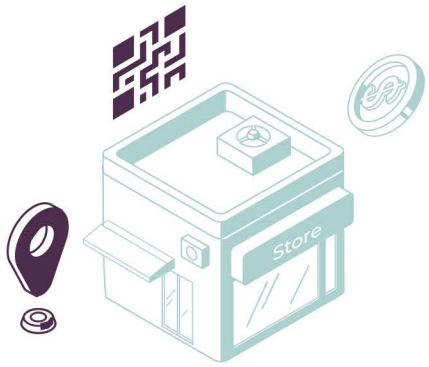
Incognia checks, in real time and in the background, whether the user is logging in at a trusted location based on their historial location behavior.

Secure QR transaction verification

To deliver the convenience promised by QR code payments, Incognia checks the user's current and historical location in real time, as well as the location of the store, to detect fraud. By doing this, Incognia helps companies detect account takeover attempts, using stolen credentials, and the use of fake QR codes. For trusted users Incognia adds no friction, such as passwords or PINs, and any high risk transactions are flagged for additional authentication challenges.

How it works

Incognia provides location intelligence to mobile apps to protect QR-code contactless payments from fraud across each of the three major use cases: In-store, Person-to-person and Remote Payments. See how it works..



In-store QR code

The customer enters the store and logs into the app

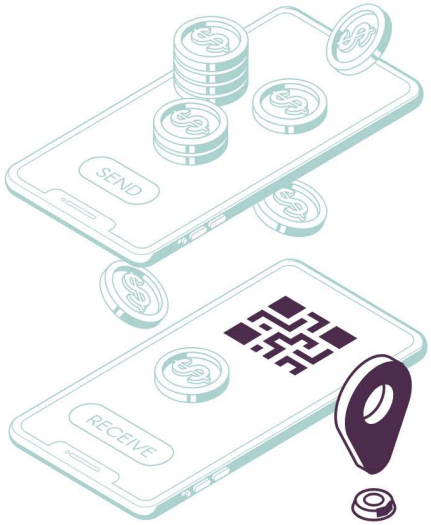
Incognia performs a device integrity check, scanning for location spoofing attempts or any other anomalies, and evaluates whether the user is at a trusted location (based on the user's historical behavior). This check detects account takeover attempts in which a fraudster has the right credentials but whose behavior is not consistent with the legitimate account owner.

The customer scans the QR code

Using AI, Incognia learns which location a QR-code is associated with to ensure that the code being scanned by the user is the one registered to that merchant. This prevents unintended payments from occurring and the resulting fake QR code fraud losses.

The payment is authorized and the customer is ready to go

If a user's current location behavior matches with their behavioral history or behavioral pattern then Incognia will deliver a low risk score, based on those location signals. If any anomalies are detected, Incognia would deliver a high risk score alerting the client to the need for step-up authentication, leaving the trusted customers with a best-in-class experience.



P2P

Both users log in to the app

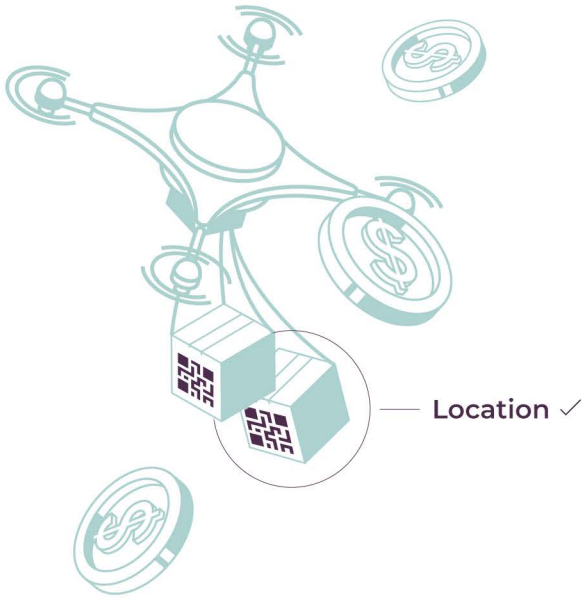
Incognia performs a device integrity check, scanning for location spoofing attempts or any other anomalies and evaluates whether both users are at a trusted location, based on each user's historical behavior, This check assesses the risk of attempted account takeovers where a fraudster has the right credentials but the location behavior is not consistent with the legitimate user

User 1 scans the QR code of user 2

Incognia verifies if both users are at the same location or at trusted locations based on their location patterns and provides a risk of any fraudulent attempt. This happens in the background, adding no friction to the users' experience.

The payment is authorized and the customer is ready to go

If a user's location behavior matches with their behavior history then Incognia will deliver a low risk score, based on those location signals. If any location anomalies are detected, our risk score can then lead those users to step-up authentication, leaving the trusted customers with a best-in-class experience.



Remote QR code payment

The customer logs in to your app

Incognia performs a device integrity check, scanning for location spoofing attempts or any other anomalies and evaluates whether the user is at a trusted location, based on that user's historical behavior. This check detects attempting account takeovers where a fraudster has the right credentials but the location behavior is not consistent with the legitimate user.

The customer scans the QR code and the payment is authorized

If a user's location behavior matches with their behavior history then Incognia will deliver a high confidence rating, based on those location signals. If any location anomalies are detected, our risk score can then lead those users to step-up authentication, leaving the good customers with a first-in-class experience.

Conclusion

QR code usage in contactless payments is seeing a surge in 2020 due to heightened customer focus on health which has created demand for touch-free and fast in-store technology. Retailers with mobile apps have the opportunity to rapidly deploy this new type of contactless payment to drive usage and transactions. Given QR code use in payment is new for many merchants and users, there are important design considerations to ensuring a safe and frictionless experience for the user. Fraud detection for QR code contactless payments needs to be real-time, and frictionless for the user, therefore location intelligence can provide an important risk signal in differentiating trusted customers from potential fraudsters. While this surge of interest in QR code payments is currently driven by health concerns related to COVID-19, the speed and convenience of this form of payment is expected to change in-store transactions permanently, with traditional wallets remaining in the purse, back pocket or at home.

Learn more

Incognia solution overview
Contactless payments fraud detection

Read the document →

Video
Frictionless QR code location verification

Watch the video →

About Incognia

Incognia is a private identity company that enables advanced mobile fraud prevention for banks, fintech and mcommerce companies. Using location-based behavioral biometrics Incognia offers frictionless identity verification and authentication. We are headquartered in Palo Alto, with teams in the San Francisco Bay Area, New York, and Brazil, where our sister company, Inloco, was founded in 2014. Inloco now has 60M+ devices leveraging its location technology.

We enable the use of anonymized location behavioral data to increase account security, reduce fraud, and deliver private location context aware services. Incognia's location technology uses network signals and on-device sensors to deliver highly precise location information. By building an anonymous behavioral pattern, unique for each user, Incognia provides location context and creates a private digital identity for account security.

Companies with mobile apps and connected devices use Incognia for frictionless user ID verification, dynamic adaptive authentication, risk assessment and fraud detection, all while protecting user privacy.

About privacy

At Incognia we use privacy by design as the foundation of our product design, implementing privacy protecting techniques from conception to the final use of our products and solutions.

The Incognia technology was designed to prevent access to information capable of re-identifying users. We encrypt and hash the location data we collect, and intentionally do not collect additional PII. This means that Incognia does not collect unique static device identifiers (such as IMEI and MAC), associated accounts (e-mail and telephone), civil

identification data (name and Social Security number), as well as sensitive data – information that reveals ethnicity,religion, political opinion, religious, philosophical, political or union entities membership or data regarding health, sex life, genetics, and biometrics.

We transform location data into an unreadable version of itself so it can still be used for security and fraud prevention purposes, with techniques like zero knowledge proof, but can't be read without an encryption key, or in certain cases, not at all. Other techniques we use include probabilistic set structure, differential privacy, and k-anonymity.

The data collected by Incognia to offer its services is collected by an Software Development Kit (SDK) which is integrated into a mobile app. Every app must present Incognia's Privacy Policy in their own Terms and Conditions of Use and Privacy Policies, informing users that data will be collected by Incognia. Once authorized, Incognia's SDK starts to collect the data without identifying users. Users can also deny data collection by opting-out and not giving consent, which disables features for them. Additionally, every app must allow users to opt-out of Incognia data collection at any time giving users ownership of their data.

The Incognia team understands the power and sensitivity of location data which is why we designed our platform with a privacy-first approach.


INCOGNIA™