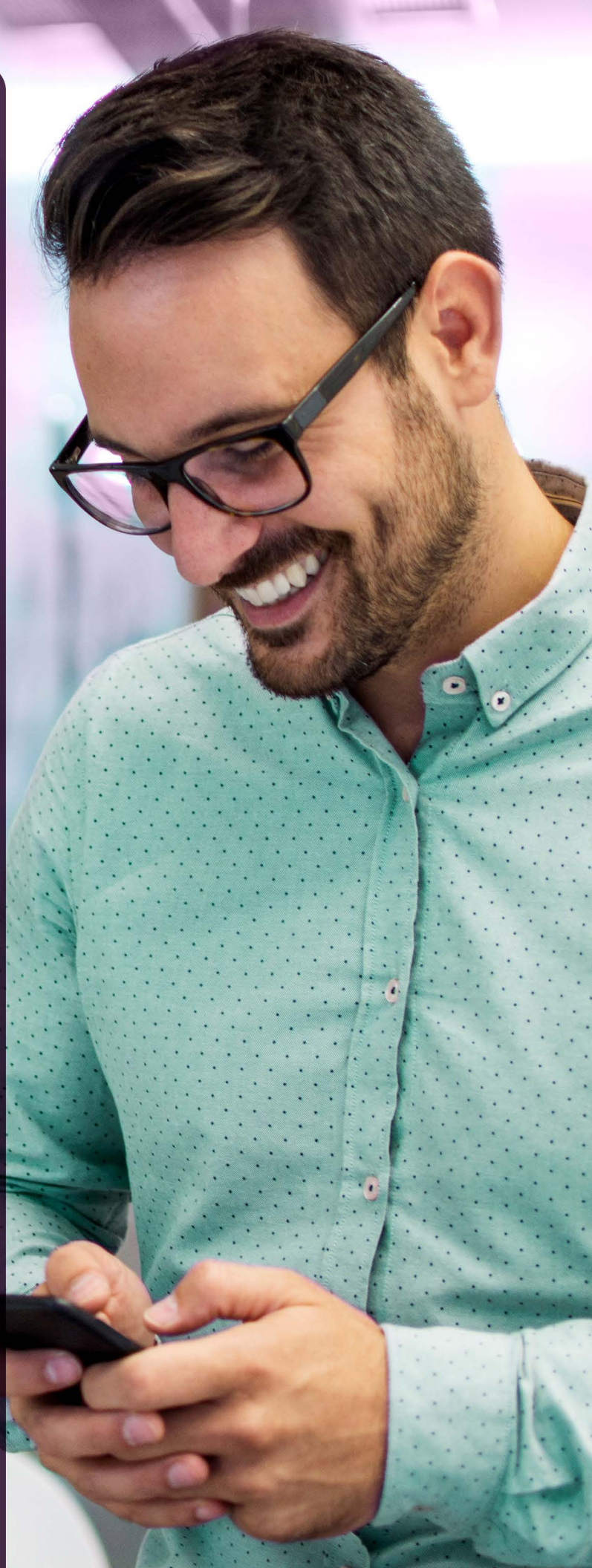
The financial services guide

Enabling frictionless fraud prevention for mobile users



INCOGNIA™

Executive summary

Business today is increasingly mobile and financial service companies of all kinds need to provide fast and efficient mobile experiences to stay competitive. These services need to be frictionless for customers while also protecting against fraud, including account takeovers and synthetic identity fraud, both of which are on the rise. With smartphone apps now accounting for the majority of digital minutes[1], predictably, fraud targeting mobile apps is increasing as cybercriminals "follow the money."

This white paper provides a review of the considerations for fighting mobile fraud while providing frictionless experiences for customers. Included is an overview of techniques that cybercriminals have developed for exploiting and defeating identity verification and multi-factor authentication. Also provided are recommendations for a new technology approach to counter these attacks that takes advantage of the inherent location characteristics of mobile devices. In today's world, we are never without our mobile phones. We take them everywhere. As a result, our movements with these ever-connected devices create a unique digital pattern or "location fingerprint." Location behavioral biometrics–that is, the anonymized representation of a person's movement patterns–turns out to be invaluable for preventing fraud and delivering fast, frictionless services for mobile customers-both high-priority goals for financial services companies today.

1 Comscore, *Global State of Mobile* (2019)

Growing business means growing mobile accounts

Business today is increasingly mobile. While some businesses might still rely on foot traffic for a percentage of their revenue, hundreds of millions of consumers now prefer to use mobile channels instead for their simplicity and convenience.

Over 96% of Americans own mobile phones. They're now the most popular way of accessing the internet and for about 20% of Americans, they're the only way of accessing the internet.[2] It's estimated that by 2025, 72% of all internet users will only access the internet through smartphones[3]. Already today, about 2.4 billion people use smartphones for financial services, and the use of smartphones for shopping and managing finances has only increased during the COVID-19 pandemic. Now, about one-third of bank customers expect to increase their use of mobile and online banking even when the pandemic is over[4].

By 2025, 72% of all internet users will only access the internet through smartphones.

Even if a customer opens a financial account in a branch or store, that customer is likely going to access their account on a mobile device. This is especially true of Generation X and Millennials – the vast majority of whom own smartphones[5].

The popularity of mobile phones has important implications for financial service companies:

Mobile channels are essential for success

Companies must be able to support customers opening and transacting through accounts on mobile devices.

Mobile channels must be secure

Companies must be able to contend with fraud vulnerabilities inherent in online financial services generally, and on mobile devices specifically.

Mobile experiences must be seamless

Whatever services companies provide on smartphones must meet mobile users' expectations for fast, frictionless experiences.

Mobile channels must be compliant

Whatever takes place in a mobile app must comply with applicable regulations, including anti-fraud regulations and data privacy regulations.

---

2 Pew Research Center, *Mobile Fact Sheet,* (June 2019)

3 CNBC, *Nearly three quarters of the world will use just their smartphones to access the internet by 2025,* (January 2019)

4 The Financial Brand, *Big Banks Benefiting Most from COVID-19 Digital Shifts,* (2020)

5 Pew Research Center, *Millennials stand out for the technology use, but older generations also embrace digital life,* (September 2019)

Challenges of mobile identity verification and authentication

Identity verification and continuous authentication are key requirements for any financial services mobile app. Companies need to be confident they know who is opening an account, who is logging into that account, and who is executing transactions associated with that account.

But identity verification and authentication on a mobile phone presents unique challenges for balancing fraud and friction.

- **Fraud prevention**
  Financial service companies need to verify new users and authenticate returning customers every time they access their account or perform a high-risk transaction.
- **Frictionless experience**
  Every mobile interaction with customers needs to be fast and frictionless so that customers don't become frustrated and click away to another website or app.
- **Compliance**
  Any identity verification practices need to comply with anti-fraud regulations such as Know Your Customer (KYC) programs and Anti-Money Laundering (AML) rules, while also respecting a customer's privacy as required by regulations such as the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Financial fraud rose 104% just in Q1 of 2020.

Of these three challenges, fraud prevention is the trickiest. Cybercriminals have more tools, techniques, and stolen data to work with than ever before, and it shows: Financial fraud rose 104% just in Q1 of 2020.[6] Companies should expect fraud to remain an important challenge in the years ahead.

While fraud prevention might be the most difficult of these challenges, all three are important and interrelated. In fact, addressing fraud in a way that increases customer friction is a losing proposition for companies. While reducing fraud losses is the goal, when security controls frustrate customers, the result is onboarding drop off, lower conversions, and ultimately, negative effects on top-line revenue.

6 *Security Boulevard, Financial fraud reports in the US jumped by 104% in 2020 Q1 (June 2020)*

Challenge #1:
Preventing fraud on mobile devices

Cybercriminals follow the money. They use automation and data to execute their crimes. Let's look at the cat-and-mouse game that financial services companies and criminals regularly play around account security on mobile devices, specifically focusing on two common attack vectors:

Synthetic identity fraud
In which criminals combine personal information from real people with fake data to create a manufactured identity for opening fraudulent accounts.

Account takeover attacks
In which criminals gain access to a legitimate customer's account and use it to steal funds or perpetrate other financial crimes.

Synthetic identity fraud

With all the personal and ostensibly private information readily available to fraud operators, it's no surprise that identity theft is on the rise. In 2019, consumers reported 3.2 million instances of identity theft to the Federal Trade Commission (FTC). Of those, 1.7 million reports involved fraud, and in 23% of those instances, consumers lost money – a total of $1.9 billion cumulatively, representing an increase of $238 million over 2018[7]. Since the COVID pandemic began, identity theft and consumer fraud rates have risen even more sharply, as fraud operators take advantage of public information to impersonate consumers eligible for unemployment insurance or other forms of government relief.

3.2 million instances of identity theft were reported in 2019.

7 Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime,* (2020)

Synthetic identity fraud is the fastest growing form of financial crime in the U.S., costing $6 billion annually according to the Federal Reserve[8]. This type of fraud occurs when fraudsters combine both legitimate and fake identity data to create a fake, "synthetic" identity. The name and Social Security number might be legitimate for one person, the address history for another, and the phone number history for someone else. Fraud operators use these elements to create a fictitious person, and then open new accounts at banks and other online businesses. They'll conduct business legitimately with these accounts for months or even years, building up a credit history with the synthetic identity for the purpose of eventually executing a transaction with a high payout. The typical payoff per incident: $10,000 to $15,000.

Synthetic identity fraud is the fastest growing form of financial crime in the U.S.

Unfortunately, this is a type of fraud that's notoriously difficult to detect. According to the Fed, commonly used fraud detection models miss synthetic identity fraud in 85% to 95% of cases[9]. Fraud prevention techniques designed to prevent account takeover–techniques such as multi-factor authentication–are largely helpless to stop fraud operators once they've applied for and been granted an account with working credentials.

Commonly used fraud detection models miss synthetic identity fraud in 85% to 95% of cases.

This costly form of fraud is most effectively stopped at account opening, but how it's stopped matters. Inconvenient and time-consuming uploads of identity verification documentation can negatively impact business growth.

8 CNBC, *Criminals are using 'Frankenstein identities' to steal from banks and credit unions,* (January 2020)

9 Federal Reserve Banks, *Payments Fraud Insights: Detecting Synthetic Identity Fraud in the U.S. Payments System,* (October 2019)

Account takeover of mobile accounts

Financial services companies and other businesses have a variety of means for guarding against account takeover fraud, yet fraud is still rising. Fraudsters continue to find ways around security defenses. Let's take a look at these defenses and why they're still coming up short.

Multi-factor authentication

To guard against the inherent weakness of usernames and passwords, many companies turn to multi-factor authentication (MFA), requiring customers to supplement their password with some other information or interaction to verify their identity. This factor might be:

- A one-time password (OTP)
  A unique, randomly generated number sent by SMS or push notification to the account holder's mobile phone, so that the customer can enter it in an online form, demonstrating ownership (or at least control) of a previously authenticated mobile device.
- A one-time code from an authenticator app
  A numeric code from a special mobile app that automatically generates a random number recognized by a website or other mobile app.
- Knowledge-based authentication (KBA)
  A question based on credit history and designed to require the customer to enter non-public information that only they would know, thus ostensibly verifying the customer's identity.

Weaknesses of multi-factor authentication

While MFA is an important step in increasing account security, and is definitely an improvement on using a user-name and password, the reality is that even MFA is being circumvented using a variety of attacks.

SIM swap fraud

SMS messages can be intercepted in a variety of ways, enabling criminals to enter secure codes intended only for legitimate customers. Perhaps the most effective way of intercepting SMS messages is to perpetrate a SIM swap.

Cybercriminals have figured out how to use social engineering to transfer account ownership from one SIM card to another. For example, a fraudster will call a telecommunications company impersonating a legitimate customer who has had their phone lost or stolen and convince a customer service agent to transfer the customer's phone number to a SIM card they own. Once the account has been transferred, phone calls and SMS messages will go straight to the criminal's mobile phone. The criminal can then use their phone to intercept SMS messages used to verify the customer's identity when locked out of an account or when changing passwords. Very quickly, the criminal can gain access to email accounts, social media accounts, and financial services accounts. By the time the fraud is discovered, funds may have been transferred and lost.

Because of the rising popularity of SIM swap attacks, security experts now discourage the use of SMS as a form of second-factor authentication altogether[10]. Even when SMS messages aren't intercepted, they sometimes arrive late or not at all, frustrating customers who are trying to log into their accounts to complete a transaction quickly and easily.

10 CNET, *Do you use SMS for two-factor authentication? Here's why you shouldn't,* (April 2020)

Authenticator app malware

Authenticator apps are more reliable and secure than SMS messages. Some, though, have proven susceptible to malware, and many are vulnerable to attacks against old operating systems[11].

Social engineering of knowledge based authentication

KBA questions have been long known to be problematic. The questions are often about previous residence, or the names of schools, pets, or teachers. But sometimes customers don't remember the right answers; another 10-15% of the time, they don't recognize any of the choices being provided, and become frustrated that they are being asked something they are not able to answer[12]. More concerning is that because of social media and data breaches, a great deal of ostensibly private information is readily discoverable by any criminal willing to do a little research. Exploring Facebook and LinkedIn, for example, will often reveal birthdays as well as the names of relatives, pets, schools, and hometowns, rendering those topics useless for fraud prevention.

Clearly, basing account security on the presumed privacy of such readily available data is a mistake. While some financial services companies still rely on KBA authentication, others are phasing out this type of authentication and seeking more reliable techniques for identity verification and fraud prevention. Ultimately, any form of authentication that relies on static information such as address histories is susceptible to error or compromise by social engineering and likely to introduce friction and frustration to customer interactions.

Biometrics

Biometrics, including fingerprints and facial recognition, are among the more recent factors being used for multi-factor authentication. While more complicated than passwords, and therefore harder to mimic or forge, unfortunately they are just as vulnerable to being stolen. Any form of static credential is problematic as an authentication credential since once stolen it can be used to take over accounts. This is especially problematic for biometrics as users do not have the option to change their physical characteristics, like they would a password.

Challenge #2:
Delivering fast, frictionless mobile experiences

Consumers have grown accustomed to quick interactions on mobile devices. If they can shop, check the weather, hail a ride service, and order a meal quickly and easily, they expect to also be able to conduct financial transactions quickly and easily.

11 Tom's Guide, *Don't run your 2FA authenticator app on these smartphones,* (February 2020)

12 Gartner, *When Knowledge-Based Authentication Fails, and What You Can Do About It,* (Setember 2012)

Financial services companies need to respect customer's time, particularly mobile customers, yet mobile interactions are often slow and frustrating. This is especially true at one critical moment: account opening. Only 8% of bank customers were able to open accounts successfully using a mobile device[13], in fact, about one in five potential customers applying for financial accounts on mobile devices abandon their applications before completing them[14]. Another study found that 40% of consumers abandon the onboarding process for financial institutions, citing the amount of time required and the amount of personal information requested[15]. The length of time required to open an account is inversely related to the percentage of customers who complete the account opening process. Research shows that adding just five minutes to the onboarding process can increase abandonment rates by 200%[16].

Only 8% of bank customers were able to open accounts successfully using a mobile device.

Adding just five minutes to the onboarding process can increase abandonment rates by 200%.

The reality is that slow, cumbersome mobile experiences are costing financial services companies valuable business. That's especially true with Millennials, who are tech savvy and interested in financial services products such as savings accounts, mortgages, and other types of loans.

> **56.3%** of all Millennials would abandon an application for a financial services product if they could not complete it on their mobile device and would switch to a more mobile-friendly competitor instead[17].
>
> **42.4%** of Millennials have left a financial services provider due to a poor mobile experience[18].

The bottom line: Whatever methods financial services companies choose to combat synthetic identity theft, account takeovers, and other types of fraud, users are not patient with security that makes account opening and other business transactions slow, cumbersome, or confusing. Customer experience is a make-or-break capability for online businesses, especially with "digital native" Millennials and Generation Z consumers.

13 Javelin Research, *Digital Account Opening Still Has a Long Road to Reality,* (February 2017)

14 Forbes *Why Can't Banks Get Digital Account Opening Right?,* (October 2019)

15 American Banker, *BankThink: Why Mobile Onboarding Is Such a Turnoff,* (July 2019)

16 Significat, Digital Banking Report (2016)

17 Mitek, *Research reveals millennial demographic "meaningless" for financial institutions and "Fintechs"* (November 2016)

18 Ibid.

Challenge #3:
Complying with data privacy regulations

At the same time that financial services companies are trying to combat fraud, there is the additional requirement to ensure compliance with a broad range of regulations, which now include data privacy regulations such as the GDPR and the CCPA. Privacy requirements vary from country to country and region to region, but in general, regulations call for:

Data minimization
Collecting only the data that is absolutely required for the business being conducted

Data security
Protecting the consumer's data from breaches and from unnecessary exposure within the organization

Data review, correction, and deletion
Enabling the consumer to request access to their data so that errors can be corrected and, upon request, data deleted if this deletion does not violate other laws and regulations

Today, 66% of countries have passed data privacy regulations, and more regulations are being drafted and discussed[19]. These laws are being written and passed in response to the public's growing concerns about data privacy, data breaches, and unwitting exposure to fraud. Over half of U.S. adults have discontinued using a product or service because of privacy concerns[20]. To earn the loyalty of customers like these, companies must take data privacy seriously.

Financial service organizations should expect data privacy to grow in importance in the coming years. Whatever security solutions are implemented to combat fraud, need to also protect data privacy.

Balance fraud, friction and compliance on mobile

There is some good news for meeting the challenges of fighting fraud while delivering fast, frictionless service for mobile users. Because customers carry their phones with them everywhere, the record of their travels provides a unique behavioral pattern or location fingerprint that can be used to verify the identity of account applicants and authenticate onboarded customers. This technological approach to fraud prevention is known as location behavioral biometrics and offers the benefit of being frictionless for users but tough on fraudsters.

Location behavioral biometrics offers the benefit of being frictionless for users but tough on fraudsters.

19 United Nations Conference on Trade and Development, *Data Protection and Privacy Legislation Worldwide,* (July 2020)

20 Pew Research Center, *Half of Americans have decided not to use a product or service because of privacy concerns,* (April 2020)

By combining signals from a variety of technologies, including GPS, Wi-Fi, Bluetooth and on-device sensors, it is possible to pinpoint a mobile phone's location to within 10 feet—an accuracy far greater than that provided by GPS or Wi-Fi locations alone.

When this location behavior is continuously anonymized, encrypted, and hashed, user privacy is protected and provides an invaluable new layer of identity verification and fraud prevention. Using location behavioral biometrics financial service companies can add an additional risk signal indicating whether or not the current location behavior of a mobile phone user corresponds with the location fingerprint for this customer.

Location behavioral biometrics at work for a mobile user

Here are examples of how location behavioral biometrics helps protect financial service companies and their customers:

New account opening

A new customer downloads a bank's mobile app and applies for a bank account, providing their home address in the process. In the background, the app calls out to a location behavioral biometrics service that compares the smartphone's location data with the address data provided by the applicant. If the applicant lists a home or work address that doesn't fit with the location data, the app will receive a high risk score indicating a mismatch. The bank can then either request more information from the applicant or reject the application outright, depending on their policies.

Multi-channel identification

A new applicant applies for a fintech account on their desktop computer at home but also has the fintech's mobile app on their phone. The applicant lists their home address and cell phone number. The web application calls the service to check the anonymized location data on the cell phone and compare it to the home address provided. If the location data matches the home address listed by the applicant a low risk score is returned indicating that the user is likely legitimate. The fintech service proceeds to open the account.

Secure transactions

A bank customer on a mobile phone attempts to transfer most of the account's funds to an account at another bank. The service determines that the location for the device being used to request the transfer doesn't match the location history of the device previously associated with the customer's profile, perhaps because the account has been compromised. The service raises an alert, so the bank can block the transfer and the bank's fraud team can contact the customer to investigate the situation.

The Incognia solution

Incognia is the industry leader in leveraging location behavioral biometrics to deliver a private identity solution for mobile fraud prevention and authentication. The Incognia solution uses anonymized, encrypted location data, captured directly from network signals and on-device sensors, to build a unique behavioral pattern that is used to identify and authenticate mobile users during onboarding, login, and transacting. Relying on dynamic behavioral data, not static personally identifiable information (PII), enables Incognia to provide financial services companies with an extra layer of security that is adaptive and private, protecting them against new fraud techniques.

The Incognia solution provides fraud protection at critical moments in the user journey:

01

Onboarding

The Incognia service compares the smartphone's location data to the address provided at onboarding. If it detects an anomalous location, the Incognia service returns a low score or no match that alerts the institution of potential risk.

02

Login

To secure existing accounts from takeover, Incognia provides a silent, background layer of security to ensure that the device logging into an account has location behavior that matches the expected behavior of that account owner.

03

Transaction

Before performing a high-risk transaction such as a high-value withdrawal or transfer, a mobile app can request a risk score from Incognia to ensure that the smartphone's current location matches the historical behavior of the device associated with the account.

While the above moments represent the most common use cases, Incognia's risk score can be leveraged according to the clients specifications. Additional use cases include a password reset, the inclusion of additional payment methods, or editing account information.

The Incognia solution offers unique benefits to financial services companies and their mobile customers:

Adaptive

- Uses real-time behavioral data for advanced identity proofing and authentication
- Creates a dynamic digital identity that cannot be predicted or spoofed

Frictionless

- Provides enhanced security without added friction
- Operates silently in the background requiring no user action

Privacy-first

- Employs proprietary location anonymization technology
- Intentionally does not collect or store any other forms of PII including names, SSNs, phone numbers, and email addresses

Integrating Incognia into mobile apps is fast and easy and usually takes less than 30 minutes. Incognia provides a fully documented Software Development Kit (SDK) and APIs. When activated in a mobile app, Incognia typically consumes less than 0.5% of battery life in 24 hours.

Mobile banking case study

By integrating Incognia into its mobile app, one of the leading retail banks was able to automatically verify 85% of all the new mobile applications it received.

38% Increase in mobile accounts opened

63% Reduction in false positives (incorrectly flagged applications and transactions)

24% Reduction in manual risk reviews saving time and money

10 False identities uncovered

Incognia helps financial services companies grow accounts, improve customer experience, combat fraud, and streamline back-office operations.

Summary

In this white paper, we have examined the mobile user requirements for verifying identities and preventing fraud while providing fast, frictionless experiences for mobile customers. We have also looked at strengths and weaknesses of security technologies applied to the mobile user, including use of MFA, authenticator apps and KBA interactions for combating fraud on mobile devices. Finally, we've considered the benefits that anonymized location behavior from smartphones can provide for improving the speed and accuracy of identity verification and authentication processes for mobile users.

Developed as a result of nearly a decade's experience with mobile location technology, Incognia gives financial services companies the fast, rigorous identity verification service they need for authenticating mobile customers and defeating fraudsters, without adding friction for the mobile customer. Incognia is a mobile security solution built for the mobile world.

To learn more about the Incognia solution ⟶

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.

Request a Demo: info@incognia.com
Learn More: www.incognia.com