INCOGNIA™

Fraud in the time of COVID-19

Staying ahead of fraudsters with new identity proofing and authentication methods

Executive Summary

This whitepaper was created by Incognia to help business leaders get a quick sense of what types of fraud risk are increasing during COVID-19 and how to best tackle the challenges ahead. The COVID-19 pandemic, and the effort to contain it, has unexpectedly accelerated digital transformation of our work and personal lives. Remote work has introduced access management issues, putting corporate information security at risk. Caught off guard by the pandemic and its consequences, businesses have quickly pivoted to ecommerce and mobile commerce, and in some cases, rapidly launching mobile apps to stay afloat. Consumers have turned to online shopping as a lifeline, buying everything from groceries to fitness equipment, safe from the virus but exposed to the risk of phishing and social engineering attacks. Additionally, the usage of digital payments and online banking apps, has spiked, now becoming the go-to solutions for transacting during the pandemic. This digital shift has brought fraud risk to the fore, as fraudsters take advantage of the chaos to execute more frequent and efficient attacks.

Companies need to acknowledge the increased fraud risk presented by COVID-19 and look to implement innovative solutions for identity verification and secure authentication that can complement and strengthen existing solutions to stay ahead of bad actors.

With the behavioral changes accelerated by COVID-19 here to stay, business and security professionals need to be aware of new threats to their organizations and customers, including mobile fraud, if they intend to stay ahead of the fraudsters.

Fraud in the time of COVID-19

Staying ahead of fraudsters with new identity proofing and authentication methods

As the first few minutes of 2020 ticked by, no one could have anticipated how quickly society would change. Threatened by a new coronavirus with no cure, every country was forced to quickly adopt social distancing and shelter in place measures. Hand sanitizers and face masks have suddenly become the norm, and everyone that can work from home has been pushed to do so. This new disease has accelerated the move to remote work and digital transactions, to enable people to minimize contact.

Companies have had to embrace working from home with record speed, and in the process have loosened security restrictions out of necessity, resulting in increased risk exposure. As people work from home on less secure networks, company data is more vulnerable to attacks. Without their office set up, security and risk professionals are dealing with the challenges of a new work environment which reduces productivity, while at the same time needing to manage increased risk.

Consumers have quickly turned to digital transactions to shop from the safety of their homes. Online purchases have grown, and not just for essentials. To comply with the social distancing rules, people have started online shopping for everything, from groceries and hygiene items, to leisure products and fitness equipment. Financial transactions of all kinds are being done digitally, accelerating the adoption of digital payments. Since COVID-19, projections for digital payments have increased, and are now expected to reach 67% of all transactions by 2025 [1].

Since COVID-19, projections for digital payments have increased, now expected to reach 67% of all transactions by 2025

[1] Bain & Company, *The Covid-19 Tipping Point for Digital Payments* (April 2020)

Cashless transactions such as contactless technology, digital payments and online banking have seen a spike in usage. In the US, Visa and Mastercard have raised their transaction limits for contactless payments [2], and other digital payments, such as Apple Pay, Samsung Pay, Google Pay and other wallet apps are seeing increased rates of adoption, as they have become the go-to alternative for safe, secure and risk-free transactions amidst this pandemic.

This sudden digital transformation is driving an unprecedented need to accelerate the adoption of new identity proofing and authentication methods to enable companies to combat fraud. Less talked about, are the challenges that new mobile financial institutions and mcommerce companies are facing to identify a huge number of new users and authenticate so many transactions at once. Considering that many businesses didn't have adequate defenses in place to score and identify fraudulent transactions, it is not surprising that mobile transaction fraud has risen considerably during COVID-19.

> “Decisions that in normal times could take years of deliberation are passed in a matter of hours. Immature and even dangerous technologies are pressed into service, because the risks of doing nothing are bigger.”
>
> Yuval Noah Harari highlights

As historian Yuval Noah Harari said in his op-ed piece in the Financial Times [3], the storm will pass and most of us will still be alive, but we'll be living in a completely different world. As society faces all these changes and deals with the various challenges of transitioning to digital channels, new risks are emerging. Unfortunately, as the world advances, so do fraudsters. They prey on chaos and vulnerability. Since the move to a work from home culture was unexpected and needed to be implemented quickly, some of it might have been done in non-secure ways. People's lack of focus and attention during this very challenging moment makes them more vulnerable to account takeover fraud, for example, initiated with phishing and social engineering scams.

Knowing this, experts should be on the lookout for new methods of identity verification. Health concerns and the rapid shift to digital have created the need to embrace new and creative ways of authenticating access. This whitepaper was created by Incognia to help business leaders get a quick sense of what types of fraud risk are increasing during COVID-19 and how to better tackle the challenges ahead.

---

[2] Oliver Wyman, *Payment Shifts with COVID-19* (April 2020)
[3] Yuval Noah Harari, *The world after Coronavirus* (Financial Times, March 2020)

Fraud is on the rise since COVID-19

Bad actors thrive on chaos and confusion. The sudden push to digital caused by COVID-19 is no exception, creating a perfect storm for fraudsters, who are finding ways to use the pandemic turmoil to their advantage. Unfortunately, fraud is expected to escalate in the weeks and months to come. As mobile and ecommerce become the dominant channels for retailers, credit card issuers and e-commerce companies are relaxing their fraud controls and increasing transaction limits in order to avoid creating friction.

Financial institutions had previously forecasted an 8% decrease in fraud in 2020 but are now projecting a 10% to 15% increase in fraud this year [4].

Considering the environment, business leaders should be on high alert for an increase in the following fraudulent activities.

[4] Aite Group, *Workplace distancing: Adapting Fraud and AML Operations to COVID-19* (April 2020)

Social Engineering Scams

Phishing attacks are on the rise during COVID-19 with fraudsters taking advantage of people being distracted. These scams are designed to manipulate people into performing an action or giving away personal information and occur on several channels, typically social media and via email. The information gained through these scams enables other forms of fraud including application and identity fraud, account takeover and card not present (CNP).

Application Fraud

During COVID-19, fraudsters are taking advantage of the confusion to open fraudulent new accounts. In this case, an attacker uses stolen Personally Identifiable Information (PII) to apply for a bank account, credit card, or personal loan. Fraudulent credit card applications are the most common type of credit card fraud in the US (88% year over year growth, as stated by Ascent [5]).

Internal Fraud

Internal fraud is always a concern during times of recession and the risk is further compounded during COVID-19 with the sudden transition to a remote workforce. Also known as occupational fraud, internal fraud is usually committed by individuals against the organizations that employ them and takes the form of theft or exposure of confidential information.

Account Takeover

A significant increase in phishing attacks during COVID-19, combined with the fact that many institutions are relaxing their identity and authentication methods in order to offer a more frictionless experience, has increased account takeover fraud. Fraudsters usually take over accounts to make purchases and/or transfer funds.

Card Not Present (CNP)

Social distancing measures implemented during COVID-19 have increased Card Not Present purchasing. Lots of people are shopping remotely - be it online, mobile or by phone - without using a physical card. Fraudsters are taking advantage of this new behavior to mix bad activity with the good.

SIM Swaps

As the usage of two-factor authentication (2FA) grows, so do circumvention techniques. SIM swapping, and SMS spoofing, are becoming more common. Fraudsters use these types of attacks to intercept one time passwords (OTP) and other account security features.

COVID-19 Stimulus Fraud

Governments around the world are rolling out coronavirus aid, relief and economic security programs to help small businesses survive the pandemic. According to security firm CheckPoint, more than 4,000 malicious websites were set up to take advantage of people and businesses looking for government support. Fraudsters are using synthetic and stolen identities to steal these subsidy payments.

Identity Theft

2019 was the worst year in history for identity theft according to Ascent [6] data. Generations X and Y are the main target, since they have more credit and tend to make more online purchases, as stated by Experian [7]. Most identity fraud is related to credit cards and other loans, but theft of personal information, such as driver's licence numbers, addresses or Social Security Numbers, are enabling new forms of identity fraud, like the creation of synthetic identities designed to bypass verification methods.

[5] The Ascent, *Identity Theft Credit Card Fraud Statistics* (April 2020)
[6] The Ascent, *Identity Theft Credit Card Fraud Statistics* (April 2020)
[7] Experian, *Identity Theft Statistics* (March 2018)

Mobile as a novel channel of attack

With the accelerated shift to digital, more transactions are occuring on mobile devices than ever before. In 2019, 53% of web traffic [8] worldwide came from mobile. Smartphone usage is no longer just reserved for games and social media, in the U.S., more than 63% of smartphone users have at least one financial app and more than 55% have at least one banking app installed.

In the U.S., more than 63% of smartphone users have at least one financial app and more than 55% have at least one banking app installed.

With so much of life today happening on mobile, it is unsurprising to see bad actors focus attacks on this channel. According to a LexisNexis report [9], mobile attacks grew 56% in 2019, while desktop attacks fell 23%, confirming the growing shift towards mobile fraud. Unfortunately, fraudsters are not only attracted to mobile due to its growing relevance but because it is still packed with security vulnerabilities. Data from Intertrust's 2020 Security Report on US Financial Mobile Apps [10] reported that 71% of U.S. financial services apps had at least one high level security vulnerability, a that can be readily exploited and has the potential for significant damage or loss. In 2019, fraud attempts increased significantly with more than two times the number of fraud attempts and an 85% increase [11] in fraud success rates. This represents a huge financial burden for financial institutions given that every 1 dollar of fraud, costs financial service firms $3.25 in losses related to transaction value, fees and investigative labor. But there is hope, Intertrust highlights that almost 70% of all high-level threats could have been mitigated using in-app protection.

In 2019 fraud attempts increased by 100% and fraud success rate by 85%

[8] Broadband Search, *Mobile vs. Desktop Internet Usage Statistics* (2020)
[9] LexisNexis, *Cybercrime Report* (March 2020)
[10] Intertrust, 2020 *Security Report on US Financial Mobile Apps* (June 2020)
[11] LexisNexis, *Cybercrime Report* (March 2020)

Attacks

+56% mobile

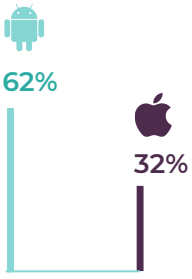
-23% desktop

Vulnerability of mobile apps

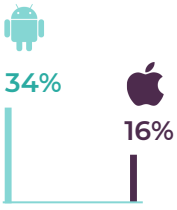
71% has at least one vulnerability

82% has weak encryption

Vulnerable to encryption key extraction



Insecure communication between apps and servers



The future is mobile so businesses need to prioritize new types of identity verification and authentication that are built for the mobile channel specifically. Mobile-first security solutions that balance friction and strong account security will be critical to avoiding the corporate and personal damage created by fraud. Two Factor Authentication (2FA) processes add a strong layer of security but their inherent friction causes users to avoid implementation. In a recent survey by Duo Security[12] only 53% of users surveyed currently use 2FA, despite the obvious security benefits. A mobile-first approach to 2FA that can work in the background, relying on user behavior to identify and authenticate access, is likely to make a bigger impact on reducing fraud given its lack of friction. Companies that offer a secure and enjoyable experience for mobile users are in the best position to prevent fraud, while protecting their business and customers.

In a recent survey by Duo Security only 53% of users surveyed currently use 2FA, despite the obvious security benefits.

[12] Duo Security, *2019 State of Auth Report* (December, 2019)

How to tackle fraud challenges

Fraudsters are always discovering new vectors of attack and learning how to capitalize on them, presenting constant challenges for security and risk experts. Luckily, new technology brings new methods of identity proofing and authentication to thwart those attacks and keep consumers and businesses safe.

While almost every security solution is hackable eventually, behavioral based identity and authentication methods have certain characteristics that make them more difficult to crack. Unlike solutions based on static credentials, behavioral biometric solutions are dynamic and continually updating making them difficult for fraudsters to predict, fake or forge.

During COVID-19 identity verification is a key challenge. Since users are not just working but also living their daily lives remotely, the ability to prove identity has become crucial for accurately onboarding customers and combating transaction fraud. For identity verification, companies usually work with third parties that rely on outdated publicly available information, often leading to false results and manual reviews that increase friction. Behavioral biometrics offers an identity verification method that matches personal information to real world behavior, and is both frictionless, requiring no documentation, and more accurate. New technology like this increases conversions and security at the same time.

For authentication, security experts strongly support the use of multi-factor authentication to secure digital accounts. Access is granted only after successfully authenticating using two or more pieces of evidence of the user that each represents either "something they know" (usually a password), "something they have" (such as a smart card or cellphone) and "something they are" (usually biometric methods, such as a fingerprint).

Today, no single method is enough to keep accounts safe. With over 7 billion records exposed in data leaks between 2018 and 2019 alone, many static credentials have been exposed. "Something you have" is susceptible to theft and "something you are" or biometric data, by far the strongest authentication factor, can be spoofed using photographs, deep fakes, and even synthetic body parts.

The key to strong authentication is to mix multiple factors and always be on the lookout for new solutions that have not yet been hacked by fraudsters.

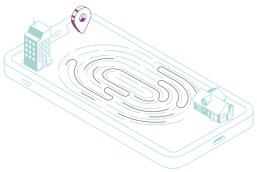
> Behavioral biometric authentication is one of the new frictionless methods used to fight fraud

By leveraging unique behavior that is difficult to fake - such as typing cadence, location behavior or even a person’s gait - authentication can benefit from an additional layer of security to keep bad actors from gaining access.

Location-based behavioral biometrics

Incognia is an example of a behavioral biometrics solution based on location behavior. Incognia uses location data captured from network signals and on-device sensors to identify and continuously validate the behavioral pattern of users. Using location patterns, rather than static personal information, means users are secured without compromising their privacy or contributing to downstream fraud in the event of a data breach. Through network signals and on device sensors, Incognia builds a unique behavioral profile for identity verification and authentication.

How location behavioral biometrics works

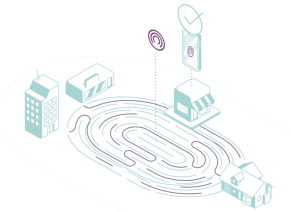


Location Fingerprint

Creates a private digital identity based on behavioral patterns unique to each user

Address Verification

Analyses location behavior to confirm if users actually live at the addresses provided during customer onboarding



Trusted Location

Verifies the location of a device in the exact moment an important in-app action takes place

Device Integrity

Detects attempts to send forged, spoofed or emulated location data to mobile applications

Key benefits of behavioral biometrics

Dynamic digital identity and adaptive authentication

Continuous real time fraud detection

Frictionless & requires no action from users

Not based on static PII

Bet on being simultaneously secure and privacy compliant

Some account security measures inadvertently invade people's privacy. User privacy has been a hotly debated topic and trend reports, such as Fjord's 2020 [13] Trends and Future Trends 2020 [14], suggest that privacy will remain central for years to come.

More than a trend, privacy is a legal concern for companies all around the world. Governments are developing regulations to enforce that their citizens' data is protected, such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the US and the General Data Protection Law (GDPL) in Brazil.

More than a trend, privacy is a legal concern for companies all around the world.

Layer security to fight fraud

Experts in risk, security and governance are aware that there is no silver bullet for secure identity proofing and authentication. As the world advances, unfortunately so do fraudsters. They prey on vulnerabilities, such as the ones the world has been facing during COVID-19. Unexpected and unsecured moves to working from home, people's lack of focus and attention to avoid scam messages and the hectic move to digital transactions, all present golden opportunities for fraudsters.

To fight fraudsters and protect companies, business leaders need to be aware that a single piece of evidence ("something you have") is not enough to guarantee safe systems. As the need for Two Factor Authentication (2FA) methods increases and users adapt, fraudsters will continue to find workarounds. Companies need to layer multiple solutions to secure digital accounts against fraud.

Companies need to layer multiple solutions to secure digital accounts against fraud.

[13] Accenture Interactive, *Fjord Trends 2020 Report* (2020)
[14] Future Today Institute, *2020 Tech Trends* (March 2020)

6 Key tips for fighting fraud during COVID-19

01

Embrace remote work and plan for it to continue.
Upgrade remote security protocols and identity and access management system for the new norm of employees working from home. Give your employees the tools they need and train them on best practices.

02

Invest in mobile-first solutions.
As smartphones become the core of digital life, be prepared to offer a frictionless method to identify and authenticate access through mobile devices. Look into mobile-first behavioral biometric solutions to protect your users from fraud.

03

Layer fraud security solutions.
Prepare for fraud attacks on a variety of fronts. While bad actors have a preferred modus operandi, they tend to capitalize wherever they see an opportunity. Get ahead of fraud with a multi tiered approach.

04

Look for frictionless transaction security.
As limits get relaxed during these challenging times, explore ways to step-up transaction security.

05

Explore new identity proofing and authentication technology.
Behavior based security solutions can be layered on top of existing fraud solutions to provide additional security and continuous risk monitoring without adding friction.

06

Put user privacy first.
Learn how new fraud methods threaten user privacy and take proactive steps to protect your organization and ensure you are in compliance with regulations, such as GDPR and CCPA.

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.

Incognia Privacy

User privacy is a central concern of 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.

Incognia technology was designed to prevent access to information capable of re-identifying users. We focus on encrypting and protecting 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.

Our goal is to transform location data into an unreadable version of itself so it can still be used, 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, bringin the data closer to full anonymization.

The data collected by Incognia to offer its services comes from the mobile device through our Software Development Kit (SDK). 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 have an internal commitment to go above and beyond in protecting user privacy.