How-to Series

Location Spoofing

5 Ways Fraudsters Spoof Location

INCOGNIA™

Location spoofing is now becoming a standard technique used by fraudsters. With access to off-the-shelf tools, fraudsters can easily defeat legacy fraud detection systems using simplistic location models based on IP address and GPS locations. By spoofing IP addresses and GPS locations, fraudsters can fool legacy risk decisioning engines.

In today's mobile world, fraud prevention requires more advanced location technology to detect location spoofing.

Incognia location technology leverages a broad set of network signals, including Wi-Fi, Cellular, GPS and Bluetooth, and on-device motion sensors to build location environments and location behavior patterns unique to each user that are extremely difficult to mimic or forge.

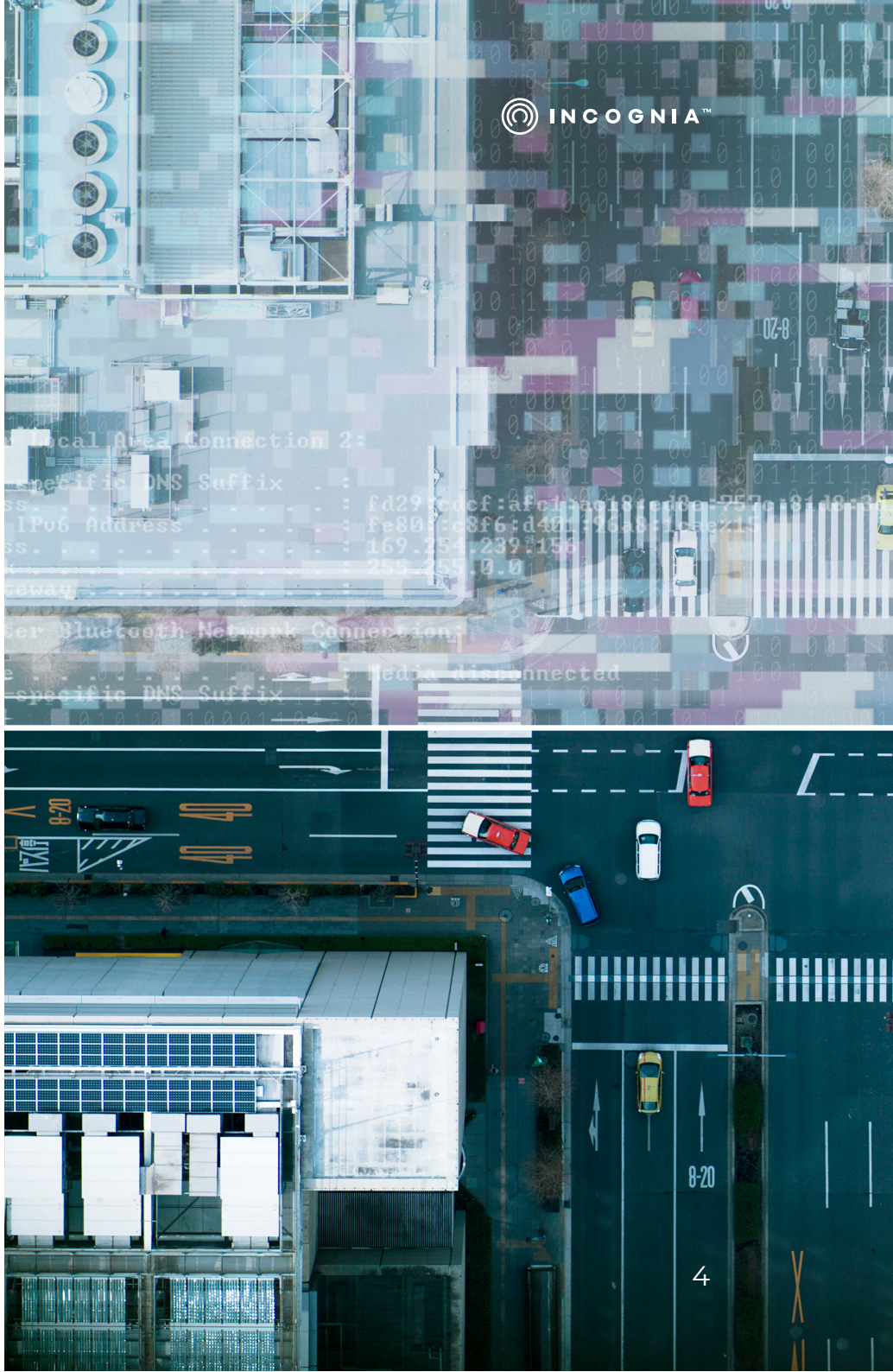
The role of location in mobile services

Today, smartphones are increasingly the go to device for transportation, navigation, mcommerce, banking and entertainment services. Many of the new mobile services we enjoy as users rely on location information. The most common location technology used by apps today are GPS or IP address however fraudsters are increasingly spoofing location and circumventing security controls based on these types of technologies.

For apps such as social networks, and dating apps, location spoofing is a serious trust and safety problem. For financial apps, location spoofing threatens the effectiveness of fraud detection systems.

Why do users spoof their location?

The primary reason why users spoof their location is to conceal their true location to circumvent some feature of an app. When the reason for location spoofing is to circumvent a security, trust and/or fraud prevention feature then fraudsters are at work. **Fraudsters do not want to reveal their true location to avoid the risk of being caught.** Most legacy fraud prevention systems leverage the IP address or GPS location as part of their risk decisioning. By spoofing IP and GPS locations, fraudsters can fool the risk decisioning engine.



Five ways fraudsters spoof location

Here is a rundown of the five most common techniques used for location spoofing:

INCOGNIA™

01

VPNs and Proxies

Fraudsters, and also many users today, use proxies and VPNs to hide their IP address through connection with a remote computer. A critical difference between a proxy and VPN is that a proxy runs at the application level, while a VPN runs at the operating system level. Most fraud prevention technologies use the IP address to locate the user's device, but the use of VPNs and proxies can easily fool these types of fraud detection systems and thereby conceal the user's true location.

02

GPS spoofing apps

After the boom of ride-sharing Apps and location-based massively multiplayer online role-playing games (MMORPGs), GPS spoofing applications have become widely available and used. These Apps not only enable gamers to fake their position to take an advantage in a game, but have also been adopted by fraudsters to mock their location to fool fraud detection systems.
Most fraud prevention technologies use the GPS location to locate the user's device, but GPS spoofing Apps can now fool these systems. Fraudsters don't even need to root their devices, or have super admin privileges to make use of spoofing apps, they just need to configure their devices in developer mode to activate GPS spoofing.

03

Emulators

Emulators are a standard tool used by developers to test mobile Apps from a computer without deploying the App into a mobile device. Emulators are also used by fraudsters to commit fraud using the emulator's powerful capabilities to manipulate the App's data. One of the data points that is easily manipulated via a mobile emulator is the geolocation information.

04

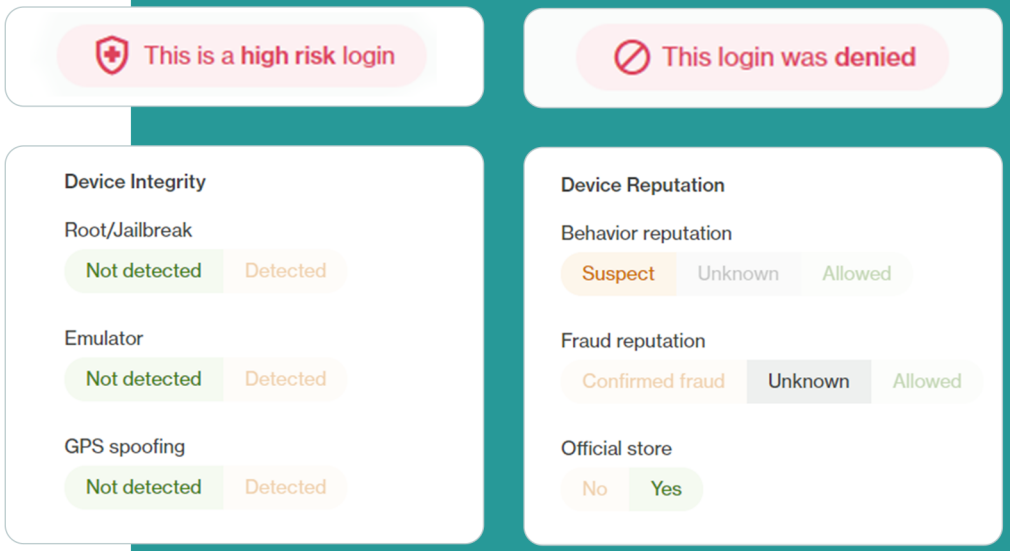
Instrumentation tools

Tools such as Frida, a dynamic code instrumentation toolkit, are primarily used by testers and developers. Fraudsters use the tool to mimic a device, and spoof location to fool fraud prevention systems.

05

App tampering

App tampering is the process of modifying the compiled code of the application. By inserting custom code into the original application, fraudsters can report fake locations. assessment.



How to protect apps from location spoofing

Given the easy access to location spoofing techniques and the increasing usage of fintech and m-commerce apps, it's time for companies to upgrade fraud detection based on GPS or IP location. Today, fraudsters are routinely fooling fraud detection systems relying only on GPS or IP address for location-based risk-assessments.

Incognia location technology uses network signals, including GPS, Cellular, Wi-Fi and Bluetooth and motion sensors to provide highly accurate location behavior intelligence that is extremely difficult to spoof. Using the location sensor data from the device, Incognia uses a number of key location behavior concepts as the basis for Incognia's location identity, that make it extremely difficult for fraudsters to fake their location and go undetected. Used in combination these location concepts establish trusted locations and location patterns for users, that are used as part of Incognia's risk-assessments.

Key Location Concepts

Location Environments

Each location has a unique signature of GPS coordinates, and available WiFi, Bluetooth, and cellular network signals. Incognia maps and correlates these signatures to create unique environments and uses this information to identify the location of a device with high precision and accuracy, even indoors.

Location Fingerprint

Each user has a unique location behavior pattern, like a location fingerprint, that comprises frequently visited locations specific to that user. As the user moves location this location fingerprint is constantly changing and updating making it extremely difficult to mimic or forge.

Trusted Locations

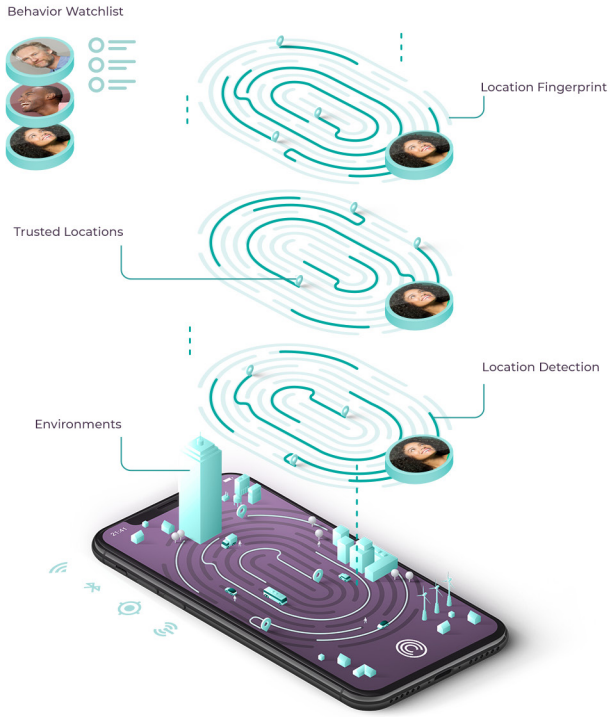
The highly frequented locations by the user and device are classified as the user's trusted locations. When Incognia detects a user is in a trusted location, there is a higher probability of the transaction being legitimate and a lower risk for fraud.

Location Detection

Incognia uses geofencing and activity recognition techniques to detect if a device has significantly displaced its position. By scanning Wi-Fi and Bluetooth signals, Incognia can detect displacements in position and confirm that the device is at a different location, or returning to an already mapped location without having to pull GPS coordinates every time. This technique also minimizes battery consumption on the device to 0.5% in 24 hours.

Behavior Watchlist

Incognia location technology is deployed in over 100 million devices providing a powerful network effect. Devices and locations that have been associated with fraud or suspicious behaviors are added to the Incognia Behavior Watchlist. As a customer of Incognia, any device or location on the watchlist will be indicated in the evidence list. This information will be used in the risk assessment.



Location Identity

5 Key Technology Concepts

Read more ⟶

What is required to enable detection of location spoofing?

In order to use Incognia location technology for fraud detection and location spoofing detection within a mobile app, Incognia is deployed as a lightweight SDK and APIs that deliver a risk-assessment with detailed evidence. Users of the app must also enable location permissions on their device.

In the network of 100 million devices with Incognia deployed we see very high rates of user opt-in for use of location permissions for the purposes of fraud prevention. Best practices on messaging for location permission show that when the description of why location is used is clear and provides direct value to the user, opt-in rates are high. If the permission request is hidden or linked to a feature that does not give real value, the acceptance percentage will be smaller.

Incognia detects location points and collects location data solely to protect the user and to prevent fraud.
For optimum performance Incognia relies on the following device features and permissions:

Location services should be turned on

The mobile device should be connected to a network

The user should provide their permission to collect location data

Read more in:

How-to Series

Location Permissions

5 Important Considerations

Learn more ⟶

How-to-Series

Location Identity

5 Key Technology Concepts

Learn more ⟶

Location permission opt-in

Based on privacy regulations, including GDPR, we believe that the user should have control of their data and be given the choice whether to share their location with apps or not, following the guidelines provided by the operating systems. It is important to reinforce that location permissions can help provide a more secure in-app experience, helping to identify cases of GPS spoofing, identity theft and other fraudulent techniques currently being used.

Consent to collect Data

Under GDPR - fraud prevention is considered a legitimate interest to collect data. When location is used to increase security and prevent fraud, an important question is often asked: “But why would a fraudster, in this case, share their location?” That is one of the reasons why data protection laws, such as LGPD and GDPR emphasize that, when preventing fraud, explicit consent is not necessary, as it is the legitimate interest of the user to remain secure. Note that although explicit consent is not required, the obligations of transparency and the rights of the data subjects must be observed. So any app should provide information in your privacy policy about the processing of device data by third parties for fraud prevention activities.

Our privacy-first approach to location

Location data can easily become very sensitive. That’s why Incognia follows Privacy by Design in the development of our solution and we intentionally do not capture, store or associate any additional PII with location data. We focus on hashing and encryption to protect the location data we collect, and other techniques we use include probabilistic set structure, differential privacy, and k-anonymity, bringing the data closer to full anonymization. For more information on Incognia’s commitment to privacy and how we follow five core pillars in the protection of location data and user privacy, read more in our ebook: Privacy by Design.

INCOGNIA™

Key Takeaways

- Location spoofing is now an increasingly common technique used by fraudsters.
- Location spoofing tools and techniques are now readily available.
- Fraud detection based on GPS and IP location technologies is no longer sufficient.
- Advanced location technology based on the concept of trusted locations and trusted location behavior is highly effective for fraud prevention and detection of location spoofing.

Get Started

Contact us to learn more about adding Incognia location and device intelligence to your mobile app to detect location spoofing.

Further reading

How-to Series

Location Permissions

5 Important Considerations

Learn more ⟶

How-to-Series

Location Identity

5 Key Technology Concepts

Learn more ⟶

How-to-Series

Location Technology

Build vs Buy

Learn more ⟶

About Incognia

Incognia is a privacy-first location identity company that provides frictionless mobile authentication to banks, fintech and mCommerce companies, for increased mobile revenue and lower fraud costs throughout the customer journey. Incognia's award-winning technology uses location signals and motion sensors to silently recognize trusted users based on their unique behavior patterns. Deployed in over 100 million devices, Incognia delivers a highly precise risk signal with extremely low false positive rates.