The Incognia Advantage

While a device fingerprint can help detect basic fraud attempts, a dedicated fraudster can easily bypass it. Incognia's solution goes beyond device fingerprinting alone and leverages location intelligence to block both basic and advanced attacks across the fraudster's journey.

Without Incognia
The fraudster's successful journey with basic device ID

The Incognia Advantage
Checkpoints where Incognia stops the fraudster

Onboarding

This user has a history of bad behavior and intends to access the platform for fraudulent purposes

01

The fraudster creates a new account on a previously banned device

Platform Secured
A basic device fingerprint built for fraud detection can identify that this device has been previously flagged and banned

Platform Secured
Incognia identifies the device as fraudulent, whether or not it was already flagged and banned in the past

02

The fraudster tampers with the device or app to appear new, using an emulator, app cloner, or app tampering tool

Platform at Risk
Only some device fingerprinting solutions can identify tampering and recognize that this is the same banned device

Platform Secured
Incognia identifies device and app tampering with our solution's Tamper Detection layer and device integrity checks

03

The fraudster utilizes image injection tools to bypass IDV or facial recognition processes

Platform Vulnerable
The fraudster bypasses liveness check with a photo from camera roll, accessing an account that isn't theirs

Platform Secured
Incognia identifies app tampering is present and prevents the fraudster from bypassing the IDV process

04

The fraudster factory resets the device

Platform Vulnerable
The device appears to be new, with no connection to the fraudster

Platform Secured
Incognia recognizes the device after factory reset by analyzing device attributes and exact location together

05

The fraudster switches to a completely new device

Platform Vulnerable
A device ID alone identifies no connection to the fraudster and the new device

Platform Secured
Incognia recognizes the fraudster across devices by analyzing location behavior for more persistent device-to-identity binding

Login

The fraudster is attempting to access an account that is not theirs

06

Fraudster logs into a user account with stolen credentials on a device not recognized by the platform

Platform Vulnerable
A device fingerprint alone can't determine if a login from an unknown device is an ATO or a legitimate new device

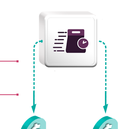
Platform Secured
Using location, Incognia is both the risk signal and authentication factor - identifying that the fraudster's location is incompatible with the account's trusted location history

07

The fraudster bypasses 2FA/basic device fingerprint and changes account security information

Platform Vulnerable
A device ID alone can't determine if a login from an unknown device is an ATO or legitimate

Platform Secured
Incognia recognizes that the fraudster's location is incompatible with the account's Trusted Locations, and the fraudster is logging in from a Suspicious Location associated with fraud



Payment

The fraudster creates both a courier and customer account and attempts to order and pay themselves with a stolen credit card

Platform Vulnerable
A device ID alone can't identify the stolen credit card

Platform Secured
Incognia identifies that the card address does not align with the account's location behavior and associates both courier and customer accounts to a single device