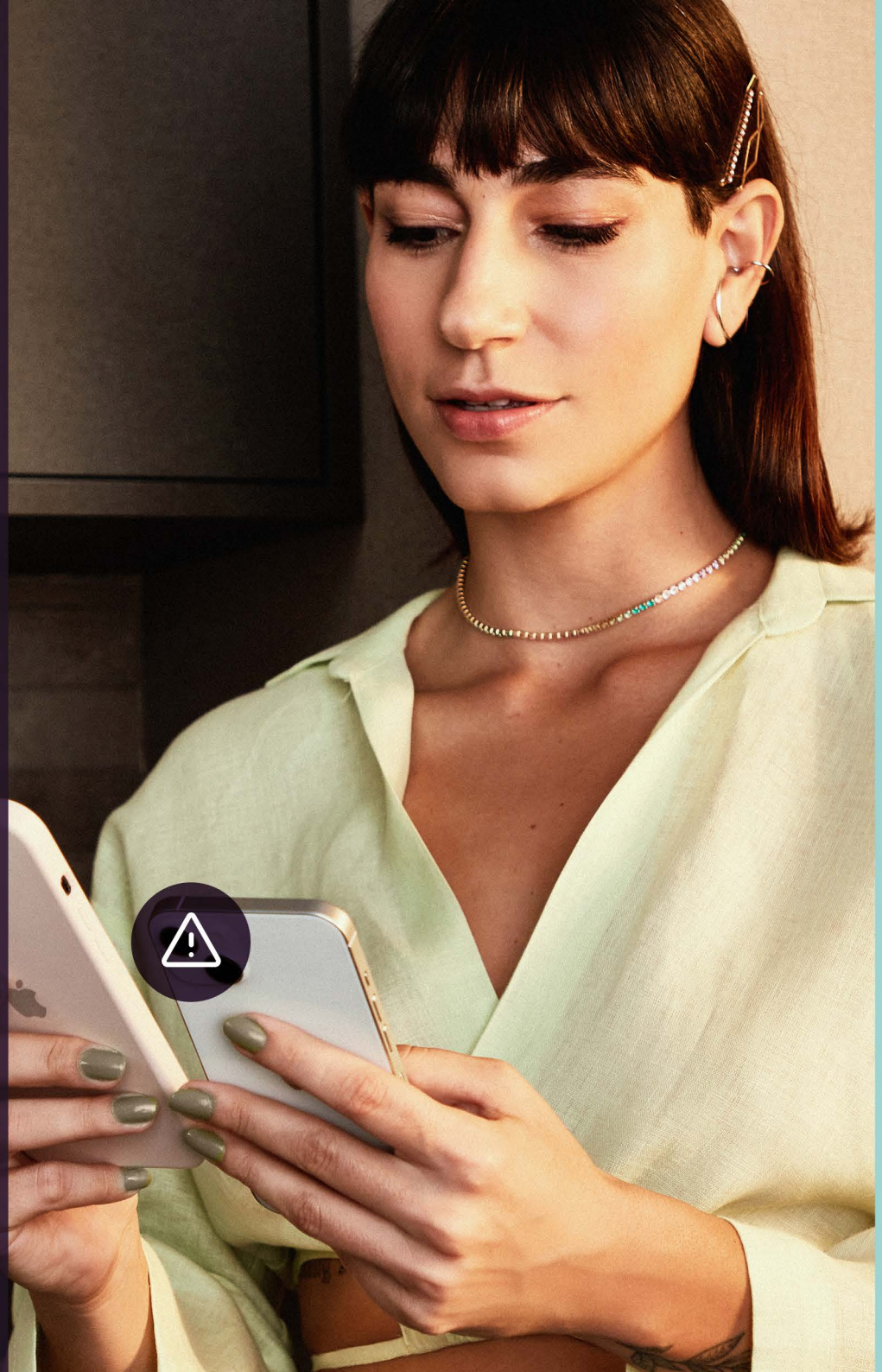
Incognia
Trust & Safety report

Policy violation & fraud

How they relate on
food delivery platforms

INCOGNIA™



Introduction

The usage and adoption of food delivery has accelerated over the past two years and has fundamentally changed how we put food on our plates. The availability of user-friendly apps for consumers and tech-enabled drivers has revolutionized the food delivery market.

Together with the convenience that these food delivery apps have brought to our lives, new types of challenges have arisen for the Trust & Safety teams of these food delivery platforms.

Trust & Safety departments have crafted “Terms of Use” policies to ensure fair use and profitable participation in this new economy. These policies have been crafted to ensure that:

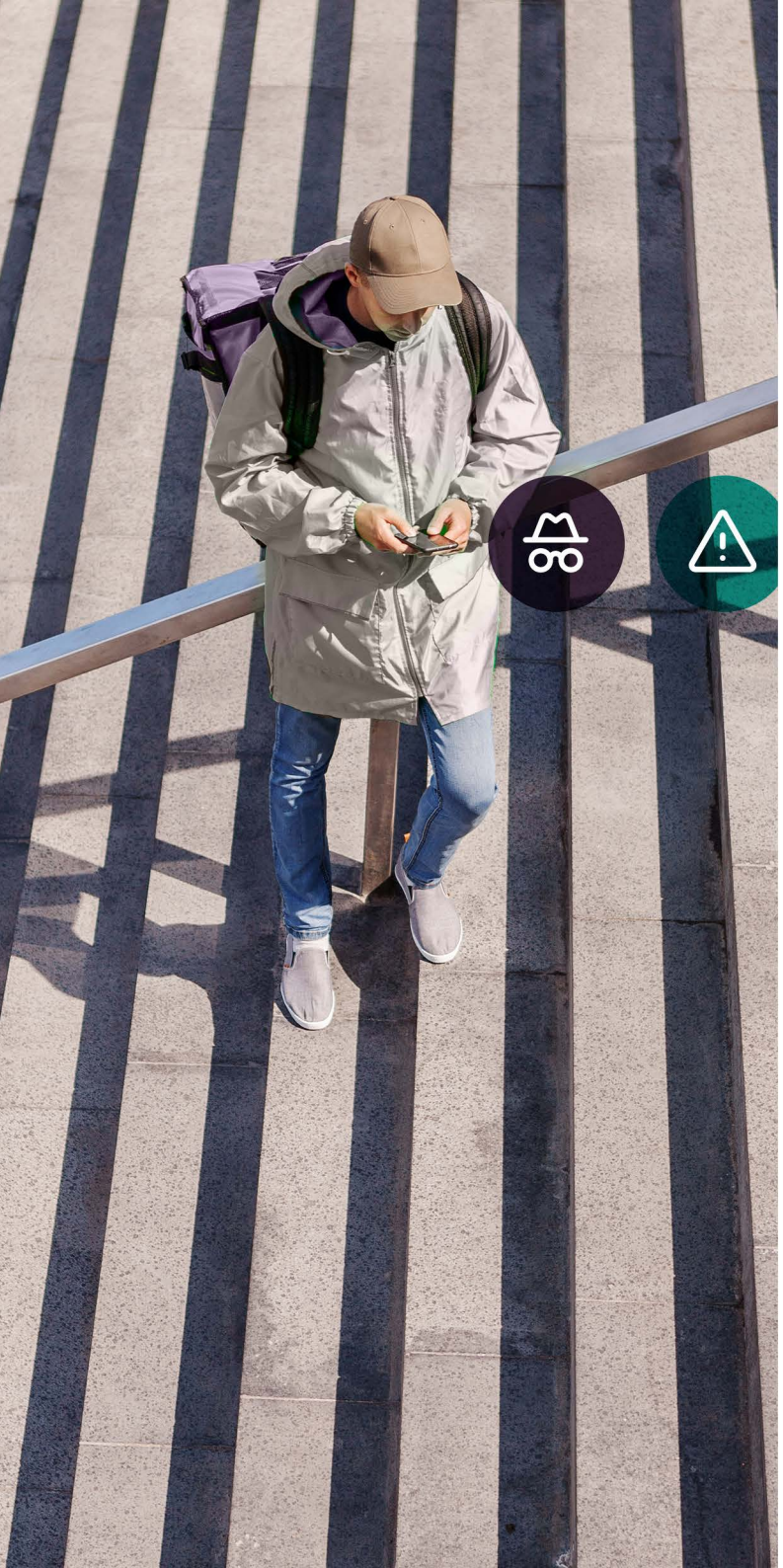
Consumers access high quality meals with the touch of a button

Couriers supplement their income by delivering meals

The Platform takes a percentage for maintaining the marketplace

However, new scams have emerged to challenge these. Bad actors take advantage of these marketplaces by abusing policies and committing fraud against the platforms, the consumers, or the couriers.

This report compares how the top four food delivery platforms address three core Trust & Safety policies. It then summarizes proprietary data from Incognia’s food delivery clients to compare policy violations on the consumer and courier apps and how they relate to confirmed fraud during the 3rd quarter of 2022.



The difference between policy violations and fraud

A “policy violation” or “policy abuse” is an act that violates a contract. Examples include violations of the “Terms of Use” of a specific product or the “Terms and Conditions” of a commercial agreement.

By contrast, “fraud” is defined by the breaking of a law: either civil or criminal. For example, “internet fraud” is defined as any type of scheme that utilizes one or more components of the internet (e.g., chat, email, app, website) to publish fraudulent solicitations, conduct fraudulent transactions, or transmit proceeds obtained through fraud.

Fraud and policy abuse are related, but not completely the same. While fraud might involve unlawful actions like account takeover and financial theft, policy abuse is using the app counter to the creators’ intentions for personal gain.

Policy violations can sometimes be a precursor to fraud; for instance, impersonating a marketplace customer service representative is a policy violation, but if a bad actor impersonates with the intention to commit account takeover and steal from users, then it becomes a fraud issue.

Today’s Trust & Safety teams lack effective tools to address policy violations. Some companies are repurposing their fraud tools to flag policy violations. While effective at detecting e-commerce fraud, these fraud tools are inadequate for identifying policy violations at gig economy companies, leaving their Trust & Safety teams underserved.

Incognia’s technology is used across multiple market segments, including food delivery, to address both policy abuse and fraud.

Trust & Safety policies in the food delivery market

Food delivery technology platforms usually utilize two different mobile apps, one for each key stakeholder:

The Consumer app is where the end user browses restaurants, orders, and pays for their food.

The Courier app is used by gig workers to accept orders, schedule their shifts, manage their wages, receive support from the platform, and verify completed deliveries. It is also common for these apps to have a mobile wallet feature through which gig workers are paid.

These two apps typically have two different “Term of Use” policies, reflecting the different Trust & Safety concerns related to each stakeholder.

Some of these policies are geography-based, changing depending on the country or state. These include specific employment policies.

However, there are consistencies between the Trust & Safety policies of the leading food delivery platforms in the world.

Specifically, this report compares how the top four food delivery platforms address several core Trust & Safety policies, including multiple account creation, account sharing, promotion abuse and device and app tampering.

The next two pages break down the relevant consumer and courier policies included in the Terms of User of each food delivery platform.

Consumer app

Policy #1: One user cannot create and hold multiple accounts

Platform A	Platform B	Platform C	Platform D
Incognia could not find any terms that specifically ban consumers from creating multiple accounts beyond what is stated under Policy #2 & Policy #3.	*"You may only create and hold one account on each of the separately branded properties on the Platforms (each, an "Account") for your personal use."*	Incognia could not find a specific ban on consumers opening multiple accounts however no two subscription accounts are permitted to use the same credit card.	*"Using multiple accounts to commit fraudulent activity is prohibited."*

Policy #2: One user cannot impersonate other users or access another user's account

Platform A	Platform B	Platform C	Platform D
"You will not use another User's account, impersonate any person or entity, or forge or manipulate headers or identifiers to disguise the origin of any content transmitted through the Services."	*"You will not access the Platform or Services using a third party's account/ registration without the express consent of the Account holder and not to attempt to impersonate another user or person"*	*"You must limit your account to your personal use, and not share your account details with any third party at any time during your subscription."* *(Pertains specifically to an account with an active subscription.)*	Incognia could not find any specific terms related to use of another user's account.

Policy #3: Users cannot abuse promotional credit, coupons or refunds

Platform A	Platform B	Platform C	Platform D
"You will not abuse our promotional or credit code system, including by redeeming multiple coupons at once or by opening multiple accounts to benefit from offers available only to first-time users."	*"Only one Trial Offer is permitted per account and per household unless otherwise permitted"*	*"Any attempt to manipulate our Site and our offers of Credits by use of bulk entry via third parties or syndicates, macros, 'script', 'brute force', masking identity by manipulating IP addresses, using identities other than their own or any other automated means (including systems which can be programmed to enter), will render the order and the relevant Credit invalid."*	*"You should not claim refund or in any way demand compensation for claims which are unsubstantiated, fraudulent, or otherwise false"*

If the platform detects any of these policy violations, it has the right to terminate and close the user account.

Courier app

Policy #1: One courier cannot create multiple accounts

Platform A	Platform B	Platform C	Platform D
"Contractor may not sign up to be a courier more than once by creating multiple accounts."	Incognia could not find any terms explicitly banning the creation of multiple courier accounts.	Incognia could not find any terms explicitly banning the creation of multiple courier accounts.	*"Do not cheat or defraud the food delivery platform by any method such as sharing or creating duplicate accounts."*

Policy #2: One courier cannot access other courier accounts

Platform A	Platform B	Platform C	Platform D
"Gaining or attempting to gain unauthorized access to the platform and/or to any account...This includes any breach or circumvention of any security or authentication measures the platform may use to prevent or restrict access to the platform."	*"You will not access the Courier app or related services using a third-party's account/registration, or attempt to impersonate another person, particularly any delivery partner."*	This platform allows drivers to elect substitutes. This means that a courier may appoint a substitute driver(s) that can use their account legally as long as they are a registered driver on the platform and adhere to certain additional requirements.	*"You may not use the Services to disrupt, interfere with, or attempt to gain unauthorized access to services, servers, or networks connected to or that can be accessed via the Services"*

Policy #3: Couriers cannot fake their true location and cannot root/jailbreak their devices

Platform A	Platform B	Platform C	Platform D
"Taking any action, either directly or indirectly, that is intended to or does damage, disable, interrupt, overburden, or impair the functionality of the Platform."	*"You will not falsely report your geographic location or prevent or otherwise attempt to prevent the Courier app from accurately reporting your geographic location."*	Incognia could not find any terms banning a driver's use of rooted or jailbroken devices, location spoofing tools, or other techniques that are commonly used to obfuscate the location of a device.	*"Couriers cannot attempt to manipulate the platform using rooted / jailbroken devices or location spoofing tools."*

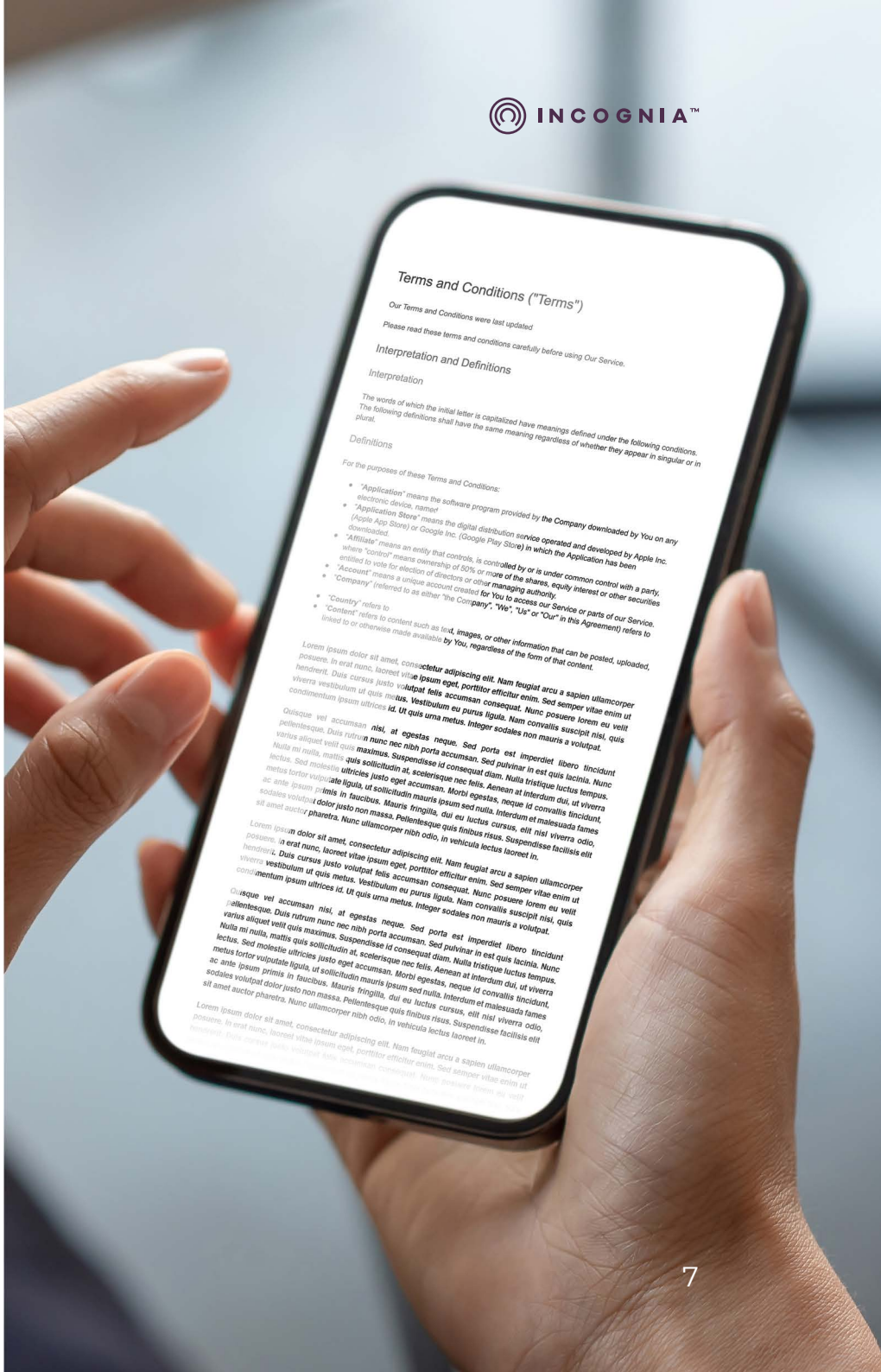
If the platform detects any policy violation, it has the right to terminate and close the courier account.

In summary, while each application's Terms of Service vary, most ban the following three actions on both the Consumer and Courier apps as they are highly correlated to fraud.

Creating multiple accounts

Unauthorized account access

Attempts to manipulate the platform for purposes known to be associated with fraud and policy violation



Why do policy violations matter?

Even though policy violations aren't illegal the way fraudulent activity is, they often represent a precursor to fraud. For example, using someone's account without their permission is a policy violation. Taking over someone's account to steal from them or the marketplace is fraud.

What's more, policy violations have all of the same power to impact the bottom line and customer experience as outright fraud does. For example, a food delivery courier could create multiple fake accounts and use location spoofing to appear as though they've attempted deliveries without ever leaving their house. It's not illegal, but the food delivery app loses money on the fake deliveries, and the affected customers have a poor experience waiting for food that never arrives. If though, the courier in this scenario claims to have completed the delivery and is paid for their work, the violation has transitioned from policy abuse to fraud. When either situation occurs at scale, it can create a serious business problem for the apps involved.

Trust & Safety policies exist to discourage bad actors, but policies alone aren't enough to stop abuse and fraud. To properly enforce their product policies, food delivery apps need the data to detect when their terms are being violated.

To properly enforce their product policies, food delivery apps need the data to detect when their terms are being violated.

Incognia insights

Data indicating policy abuse and fraud on food delivery apps in 3Q22

Incognia, a digital identity company, has created a spoof-proof Location Identity that helps Fraud and Trust & Safety teams detect policy violations and block bad actors from committing offenses. Incognia solutions have been deployed in over 200 million devices across multiple market segments, spanning financial services, food delivery, gaming, and social media.

Today, Incognia partners with several global food delivery apps to prevent payment fraud and promotion abuse on the consumer app and identify location spoofing and fake account creation by couriers.

In Q3 2022, Incogna analyzed the activity of over 58M devices running both consumer and courier food delivery apps across several different customers to understand whether widespread policy violations were occurring.

53M
Consumer users

5M
Courier users

During this timeframe, Incognia detected hundreds of thousands of policy violations and behavior commonly associated with fraud on both application types.

During this timeframe, Incognia detected hundreds of thousands of policy violations and behavior commonly associated with fraud on both application types.

Consumer app

Below is a list of the policy violations detected by Incognia in 3Q22 and a description of how each may contribute to fraud.

Consumer Policy #1: One user cannot create and hold multiple accounts

118,000
Devices accessing five or more accounts

A device accessing more than 5 accounts, is a strong indication that the user is violating the "one user per account" policy.

Bad actors typically create multiple accounts to:

- Request fraudulent chargebacks by falsely claiming food was never delivered
- Use stolen credit cards to commit Card Not Present (CNP) fraud
- Violate Consumer Policy #3, promotion abuse, by creating multiple new accounts

Consumer Policy #2: One user cannot access another user's account without explicit consent

72,000
Accounts accessed by more than 5 devices

An account accessed by more than five devices indicates that bad actors are:

- Creating shared accounts to commit credit card fraud
  - Fake consumer accounts are used to test stolen credit cards and result in chargebacks.
- Taking over accounts to steal credentials, personal information, or credit card information

While the apps covered in this report do not have terms explicitly forbidding consumers from accessing the app with modified devices, these measures are considered suspicious by experts in fraud and risk.

12,000
Devices with location spoofing

Location spoofing tools are typically leveraged by users trying to hide their true location for:

- Testing stolen credit cards
- Refund fraud
- Account Takeover fraud

70,000
Devices rooted / jailbroken

34,000
Devices running emulators

Modifying a device by rooting, jailbreaking or using an emulator is used to:

- Fool basic device detection techniques to remain anonymous
- “Clean” or disguise devices previously used to commit fraud

Courier app

Below is a list of the policy violations detected by Incognia in 3Q22 and a description of how each may contribute to fraud.

Consumer Policy #1: One courier cannot create multiple accounts

18,000
Devices accessing five or more accounts

Couriers can create and hold multiple accounts to commit fraud, such as:

- Abuse of courier sign-on bonus programs
- Fraudsters can create multiple accounts and sell or rent them on the dark web.

Consumer Policy #2: One courier cannot access other courier accounts

19,000
Accounts accessed by more than 5 devices

Couriers can create and hold multiple accounts to access unfair advantages and commit fraud, such as:

- Sharing and renting accounts to unlock or access higher status
- Taking over accounts to defraud couriers of their earnings.

Consumer Policy #3: Couriers cannot attempt to manipulate the platform using rooted / jailbroken devices or location spoofing tools

18,000	16,000	2,000
Devices with location spoofing	Devices rooted / jailbroken	Devices running emulators

Courier may spoof their location to access unfair advantages or to commit the following types of fraud:

- Gaining priority in order queues
- Accepting deliveries from busy locations
- Charging for deliveries not made
- Reporting longer rides to earn more from the platform

Couriers might root / jailbreak / emulate their devices:

- to commit social engineering
- to “clean” them by wiping away identifiers of past fraudulent behavior

INCOGNIA™

Learn more

To learn more about location spoofing techniques, download the Incognia ebook: **5 ways fraudsters spoof location**

Read more ⟶

Conclusion

In summary, **Incognia detected hundreds of thousands of Trust & Safety policy violations on both consumer and courier apps in 3Q22.**

The data depicted on previous slides and summarized to the right shows that devices running courier apps are multiple times more likely to violate platform policies.

Devices using the Courier app are 194x more likely to conduct app tampering than devices running the Consumer app

App Tampering is any unauthorized apk source code modification, such as app cloning, recompiling, and reverse engineering.

Internal data

INCOGNIA™

Consumer app Courier app

Devices using the Courier app are 3 times more likely to **open multiple accounts** than devices running the consumer app

Accounts on the Courier app are 7 times more likely to be **accessed by multiple devices** than accounts on the consumer app

Devices using the Courier app are twenty times more likely to **use location spoofing** technology than devices running the Consumer app.

Devices using the Courier app are three times more likely **to be rooted** than devices running the Consumer app.

Emulators are used at the same rate by consumer apps as by courier apps

Incognia then took the analysis one step further to compare the patterns of policy abuse to the instances of confirmed fraud on both consumer and apps.

The first observation is that the use of an emulator is over 327x more common on consumer devices associated with confirmed fraud than courier devices associated with fraud. This is likely due to the fact that emulators aid in the creation of fake accounts, which are used by bad actors to commit voucher abuse and Card Not Present fraud.

Second, app tampering is 391x more common on courier devices associated with confirmed fraud than on consumer devices associated with fraud. This high correlation is also expected given that many fraud scams that occur on courier apps require modification of app source code to manipulate information and bypass security flags.

This correlation is also expected given that many fraud scams that occur on courier apps require modification of app source code to manipulate information and bypass security flags using fake data.

Confirmed fraud is based on customer feedback delivered to Incognia via the Feedback API.

Emulator use is

327x more

common on consumer devices flagged for fraud.

App tampering is

391x more

common on courier devices flagged for fraud.

In conclusion, although devices running food delivery courier apps are more likely to violate Trust & Safety policies, not all of these violation patterns lead to more fraud.

The data shows that the policy violations that have the highest correlation with fraud differ between the courier apps and consumer apps.

- Devices running the consumer app are more likely to be associated with confirmed fraud if they are using an emulator or are rooted / jailbroken
- Devices running the courier app are more likely to be associated with confirmed fraud if they show signs of app tampering

Trust & Safety and fraud teams should ensure they have access to device integrity and confirmed fraud data from both consumer and courier devices in order to put proactive fraud prevention rules in place.

	Common policy violation	Correlation with fraud
Consumer app	App Tampering	Low risk
	Root / Jailbreak / Emulator	High risk
Courier app	App Tampering	High risk
	Root / Jailbreak / Emulator	Low risk

INCOGNIA™

Learn more

To learn more about the use of Incognia location spoofing detection visit our online resources hub.

View resources ⟶

Report
Fraud Insights Report
Food Delivery Edition

Read now ⟶

Solution Brief
Location Spoofing Detection

Read now ⟶

About Incognia

Incognia, a digital identity company, has created a spoof-proof Location Identity to silently authenticate customers throughout their digital journey. Fraud and operations teams at food delivery, ride-sharing, social media and eCommerce marketplace companies use Incognia to authenticate trusted users without friction and detect suspicious behavior to prevent new account fraud and ATO. Today, Incognia's network includes over 200M devices globally.

Incognia is a venture-backed company headquartered in California, with teams in New York and Brazil.
Stay connected and follow Incognia on Twitter and LinkedIn. **Visit Incognia.com to learn more.**