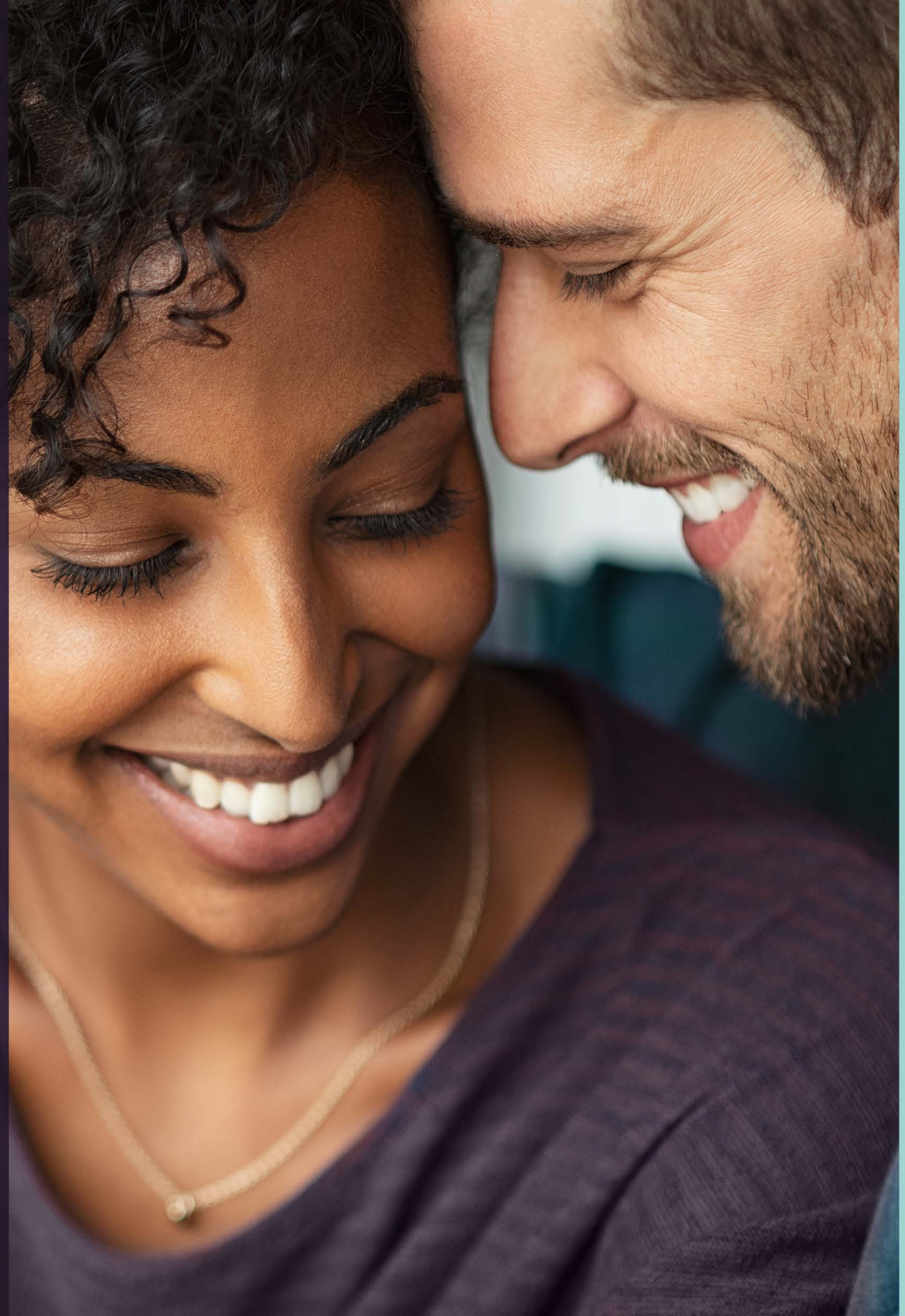


Incognia Mobile App  
Location Spoofing Report

# Dating Edition

2022



# Introduction

The growing adoption of smartphones and easy availability of GPS technologies is driving the growth of location-based apps. Dating apps are one of the major categories of location-based apps, with over 323 million users worldwide, generating \$5.61 billion in revenue in 2021. The U.S. is one of the major markets for dating apps with 53 million users<sup>1</sup>, and in 2020, **3 out of 10 U.S. adults said they had used a dating app**, according to Pew Research.<sup>2</sup>With the COVID-19 pandemic the usage of dating apps has only increased.

At the same time that users are looking for love using dating apps, fraudsters also have their eye on this growing opportunity. With easy access to location spoofing techniques and tools, fraudsters are exploiting social engineering to take advantage of dating apps to commit romance scams. The Federal Trade Commission reported **in 2021 romance scams reached \$549 million in the U.S., up 80% from the prior year.**<sup>3</sup> Fraud on dating apps not only represents potential financial losses to individual users and the dating company, but also represents a threat to user trust and safety.

Using fake identities, and by obscuring their real location, fraudsters are “catfishing” victims on dating apps and scamming them into sending money. **Use of fake locations is a key indicator on whether a user is a real potential suitor or a potential fraudster. Fraudsters never share their real location** and in the case of dating apps give every reason for not meeting in person as they exploit victims for financial gain.

Today, location and device intelligence is being used for fraud prevention on mobile apps. This report includes results from a recent study by Incognia on the state of location spoofing in 24 leading dating apps around the world.

---

<sup>1</sup> Business of Apps - [Dating App Revenue and Usage Statistics 2022](#) (July 2022)

<sup>2</sup> Pew Research - [The Virtues and Downsides of Online Dating](#) (February 2020)

<sup>3</sup> FTC - [Data Shows Romance Scams Hit Record High](#) (February 2020)

North America

---



EMEA

---



APAC






---



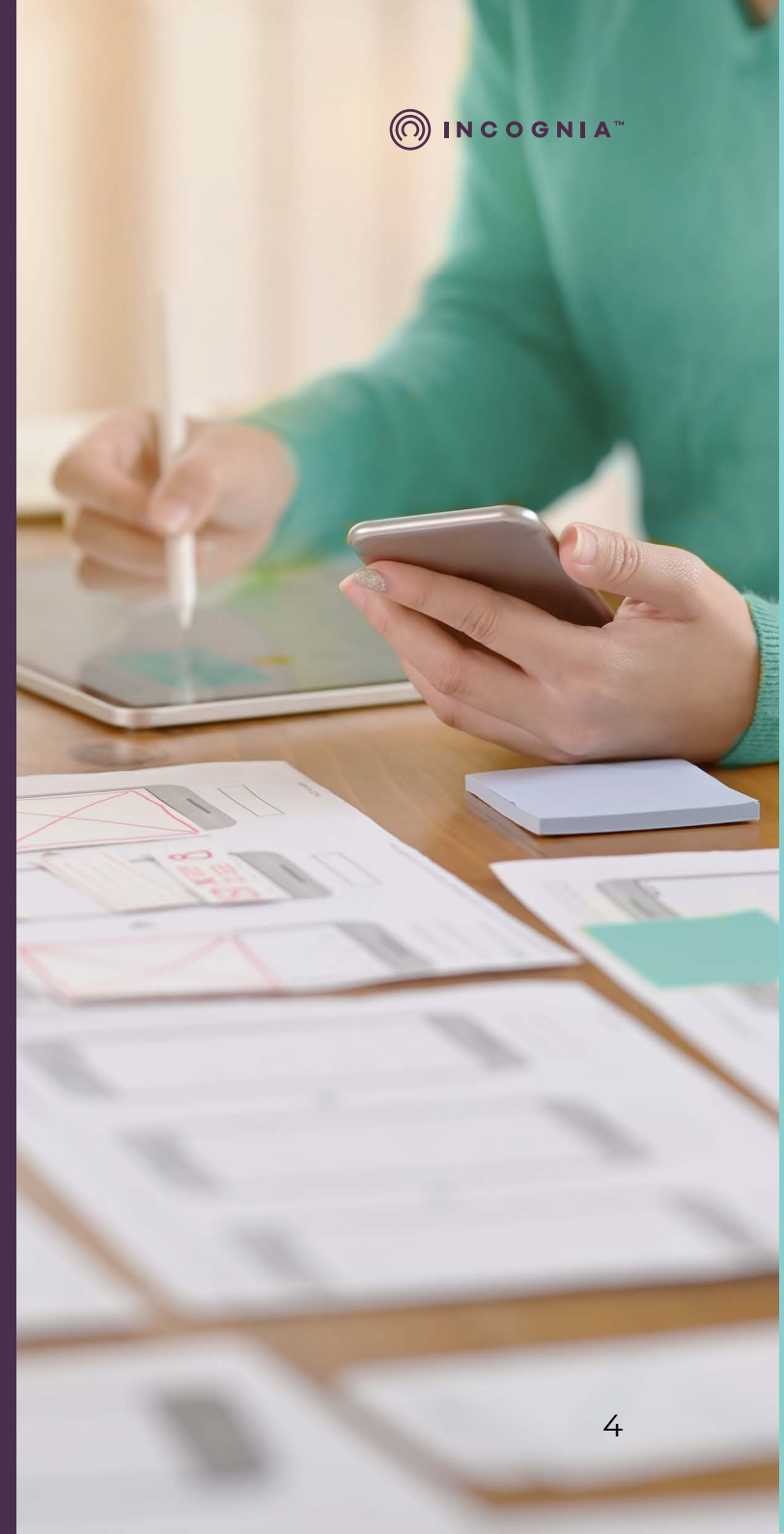
# Methodology

All tests were performed on Android versions of the apps. We tested Android Apps since there are many free apps available on the Android platform to spoof GPS location, and we wanted to test app susceptibility to the least sophisticated location spoofing approach. Testing was performed during the period from July 11 to July 22, 2022. Tests were performed by the same person using the same Wi-fi connection, to eliminate behavior and internet speed variability during the process.

The following methodology was used in testing each app:

-  Download the app
-  Create a new user account
-  Observe if the app displays the user's current real location or static location information associated with the user's account
-  Spoof the user location using a GPS spoofing app
-  Observe if the app detected the spoofed location or real location

\* Disclaimer: Mobile apps are frequently updated, and Incognia has no control over the dates of these updates. It is possible that since the publication of this report, some information may have changed as a result of the publication of a new app version.

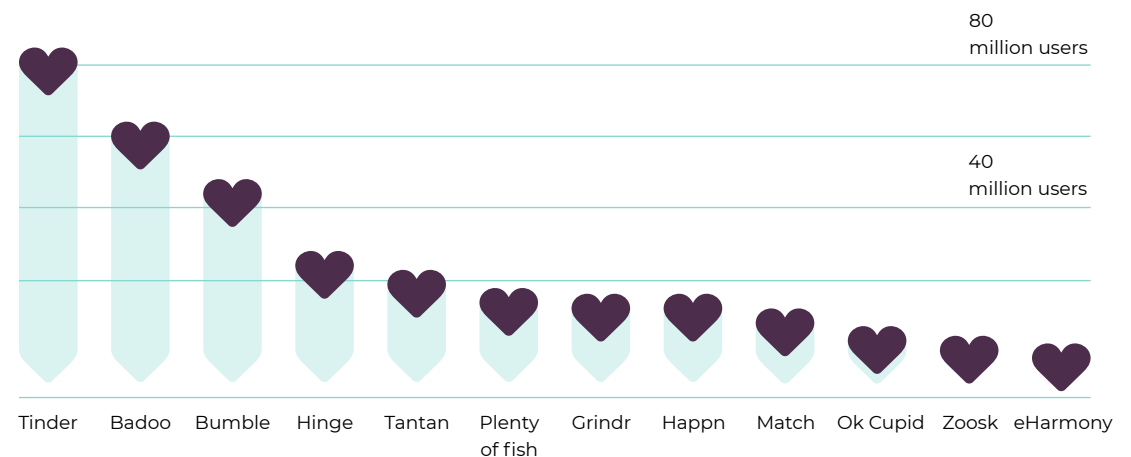


## Market background

Finding love and a romantic partner in today's world is now a digital adventure, with 3 in 10 U.S adults reporting they have used a dating app according to a 2020 Pew Research Study. Dating apps allow people to create profiles and search for their soulmate online. The use of location within the dating app is an essential feature for finding matches. For some apps such as Tinder, Happn, and Bumble, location is a key filtering tool that provides the starting point for finding matches. In some apps it is the real-time location of the user that is used, in other apps there is the feature for the user to select a location and find matches in that location.

### Most popular dating apps

In 2021, the most popular dating app is Tinder in the U.S. with over 80 million users, followed by Badoo, in Europe with 60 million users.



Source: [Business of Apps: Dating App Revenue & Usage Stats 2022](#)

## Use of location as a key filtering tool

A common feature of dating apps is the use of user location as a key filtering tool or the starting point for finding a match.



Focus on proximity of users to suggest matches.

## Hinge

Hinge allows users to pick a location to look for matches.

Users are asked to share their location for matching with potential suitors in the same vicinity. [The easy accessibility to location spoofing tools makes it critical for dating apps to detect location spoofing](#) to ensure that a user's location is real and can be used legitimately as the basis for potential dating matches.

**The easy accessibility to location spoofing tools makes it critical for dating apps to detect location spoofing.**

## From online to offline dating

Dating apps are designed to help people connect online with the goal of meeting offline in real life. When users spoof location they are not only spoofing their location online but also offline. Fraudsters committing romance scams always have a reason why they cannot meet in person. The FTC provides information for consumers on [how to be on the watch for romance scams<sup>1</sup> including the excuses fraudsters provide](#) on why they cannot meet:



Working on an oil rig



In the military



A doctor with an international organization

<sup>1</sup> FTC - [What you need to know about romance scams](#). (July 2019)

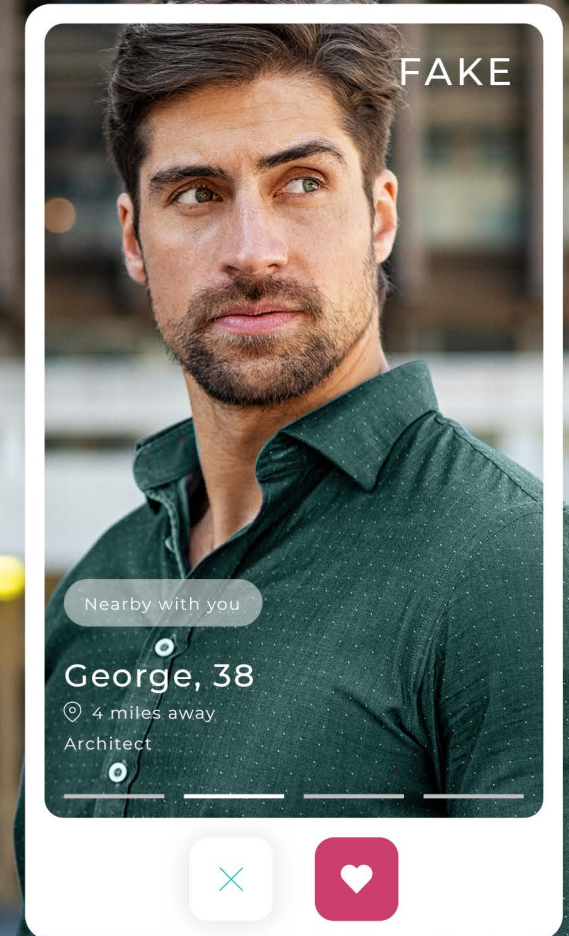
## Catfishing

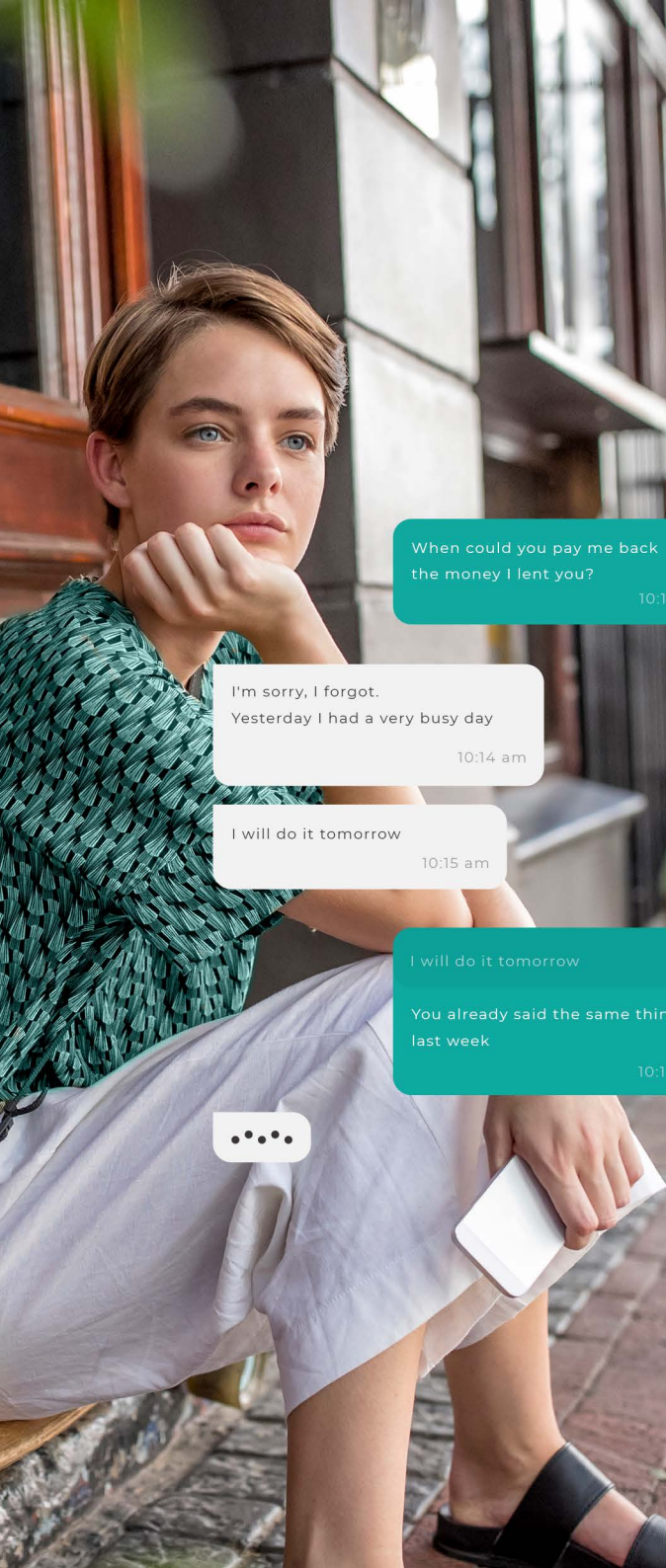
While 98% of dating app users claim to be truthful, 30% of women, and 38% of men say they have been “catfished”, by users pretending to be something they are not. In 2020 more than 23,000 US citizens reported being a victim of catfishing. The term “catfish” was popularized by the 2010 American documentary Catfish which covers the story of a man who thought he was cultivating an online relationship with a 19-year-old girl from the Midwestern United States, who instead was actually a 40-year-old housewife. The original documentary has turned into a “reality” TV series.

Why the term “catfish”? It is believed to date back to the 1900s when catfish were shipped with cod. The catfish is an enemy of cod, and would chase the cod around the tanks during shipping and keep it alive. The connection being that a fraudster or “digital catfisher” will chase their victim.

Catfishing is however not limited to just dating apps. It is a deceptive activity used on any type of social networking service where a person creates a fake persona and then targets a specific user with the goal of either financial gain, or to compromise the victim.

While 98% of dating app users claim to be truthful, 30% of women, and 38% of men say they have been “catfished”, by users pretending to be something they are not.





When could you pay me back the money I lent you?  
10:13 am

I'm sorry, I forgot. Yesterday I had a very busy day  
10:14 am

I will do it tomorrow  
10:15 am

I will do it tomorrow  
You already said the same thing last week  
10:18 am

⋮

## The cost of romance scams

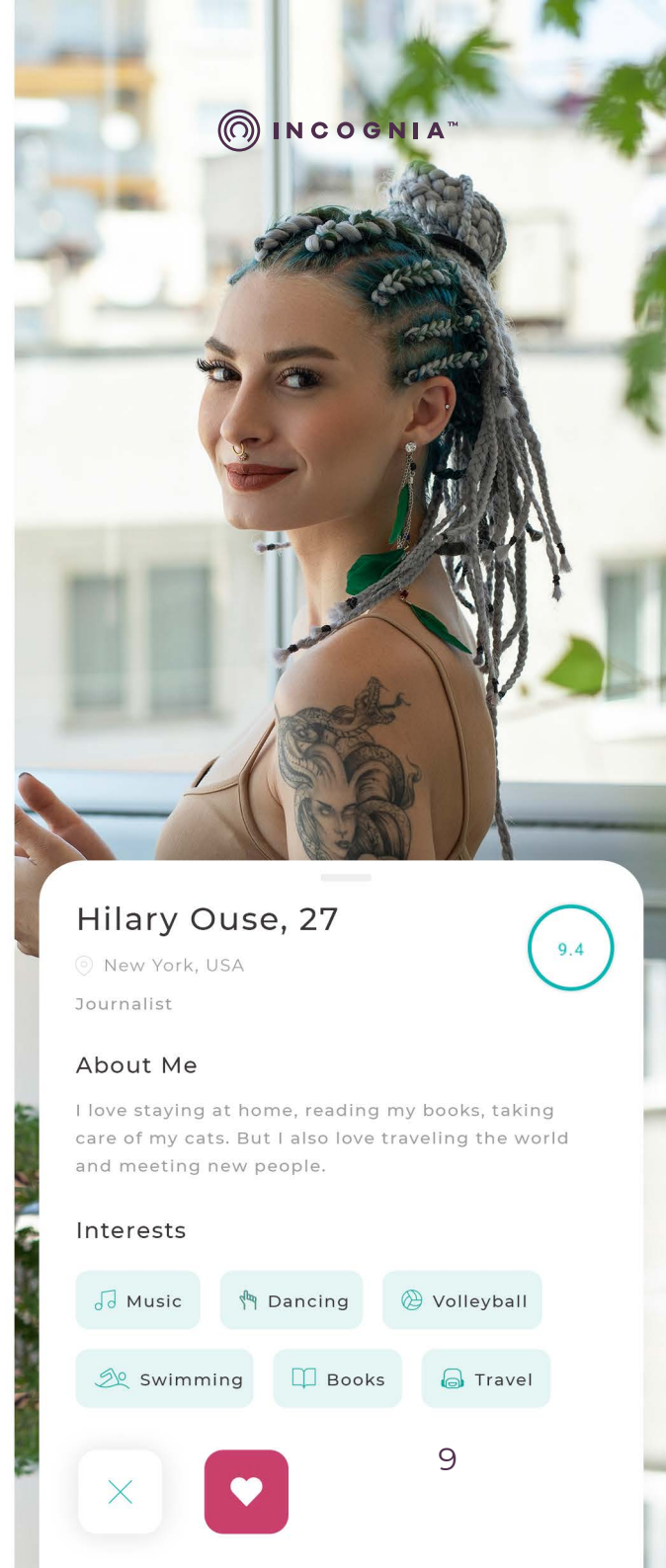
Romance scams rely on fake personas built using stolen images, using fake locations and other background details. Fake profiles on dating apps are designed to seem almost real, with the intention of drawing in the victim. The key difference between a real suitor and a fraudster, is that a fraudster always has a reason to not meet in person. Eventually, the fake suitor will ask for money from the unwitting user, with a median fraud loss of \$2,400 reported to the FTC.

The most common method (in 25% of the fraud cases) that victims use to send money to fraudsters is via gift cards. More recently fraudsters have looked to cryptocurrency to increase their returns. The FTC reports that when cryptocurrency is involved in a romance scam the average fraud losses increase to close to \$10,000.

In cases where the fake suitor does want to meet in person, the user is vulnerable to not only financial losses but also personal safety.

■ Eventually, the fake suitor will ask for money from the unwitting user, with a median fraud loss of \$2,400.





## Protecting against romance scams

Protecting users against romance scams is critical for dating apps to maintain trust and safety for users and also to avoid damage to brand reputation. [Verifying the identity of users is critical, including whether they are faking their location.](#)

Users of dating apps should be aware of catfishing and romance scams and should take steps to protect themselves. The FTC provides users with useful information and tips to avoid romance scams<sup>1</sup> including:



Ask questions and look for inconsistent answers



Talk to someone you trust about your love interest



Use an online reverse image search to find out if the person's photos are on anyone else's online profiles

**Verifying the identity of users is critical, including whether they are faking their location.**

<sup>1</sup> FTC - [What you need to know about romance scams](#) (July 2019)

Hilary Ouse, 27

9.4

New York, USA

Journalist

### About Me

I love staying at home, reading my books, taking care of my cats. But I also love traveling the world and meeting new people.

### Interests

Music

Dancing

Volleyball

Swimming

Books

Travel



9

# Summary of results

We tested 24 of the leading dating apps around the world.

**80%**

of the tested apps requested the user to share location. None of the apps provided messaging that the user location was being used for fraud prevention.

**37%**

of the apps that requested location could be GPS spoofed.

**50%**

of the apps in North America and APAC could be GPS spoofed. Of the three Indian apps that were tested, two out of three could be GPS spoofed.

None of the tested apps from EMEA could be GPS spoofed.

**% of dating apps  
GPS spoofed**

**50%**  
North America

**0%**  
EMEA

**50%**  
APAC



You've seen all potential matches in your area.

## Location details

### How do dating apps determine location?

Location-based apps make use of a smartphone's built-in sensors and technology to "locate" a user. The most commonly used technology used for determining a location on a smartphone is Global Positioning System (GPS) technology. GPS relies on signals broadcast from a constellation of satellites and is accurate to about 20m outdoors. Inside buildings, WiFi and Bluetooth signals are used for greater location accuracy. Other signals that are used for location but with less accuracy are use of signals from Cell networks and IP addresses.

Read more about location technologies in this infographic

[View Infographic](#) →

### Why is location spoofing possible on a dating app?

Location spoofing by fraudsters is the unintended consequence of providing developer support within the operating system (Android and iOS) for testing out user location. iOS and Android operating systems enable location to be spoofed as part of the developer support. In this way developers can test out their location-based services with different locations. For example a developer can test out the app for different cities and countries, without having to physically be in all these different locations.

## What are the consequences of location spoofing?

### 01

Potential revenue loss to the dating company

### 02

Financial theft in the form of romance scams

### 03

Poor customer experience

### 04

Trust and safety issues

### 05

Brand and reputation damage for the dating company

## The five main methods fraudsters use to spoof location are:



VPNs and Proxy servers



GPS spoofing apps



Emulators



Instrumentation tools



App tampering

## How is location spoofed?

There are several methods, of varying complexity, that fraudsters use to spoof location. The easiest method available to spoof location is to download a free GPS spoofing app from the Android app store. This is the method used in this Incognia study, in part to see just how easy it was to spoof an app.

Use of a location spoofing app requires no specialized developer skills. Many users also make use of virtual private networks (VPNs) to conceal their true location. Other methods that require more specialized developer skills include rooting or jail-breaking a device to manipulate the device, or using a mobile emulator to fake different characteristics of the device.

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

Read now →

## Detailed results

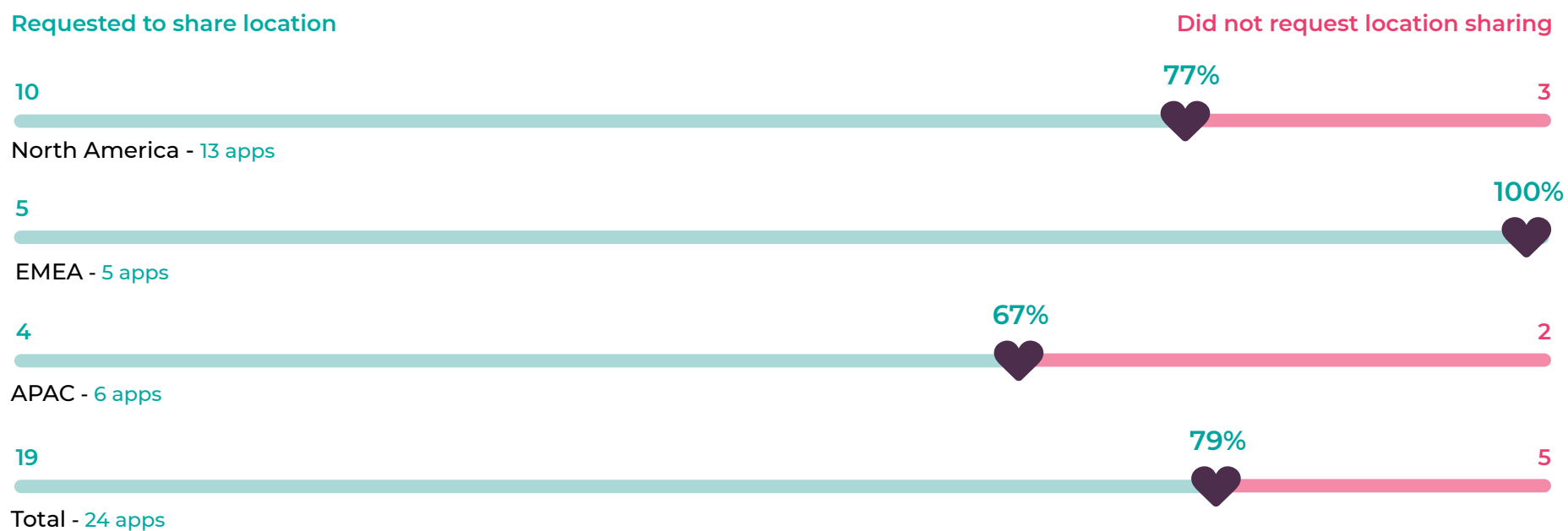
A total of 24 apps were tested as part of the Incognia Location Spoofing Study of Dating Apps.



## Requesting user to share real-time location

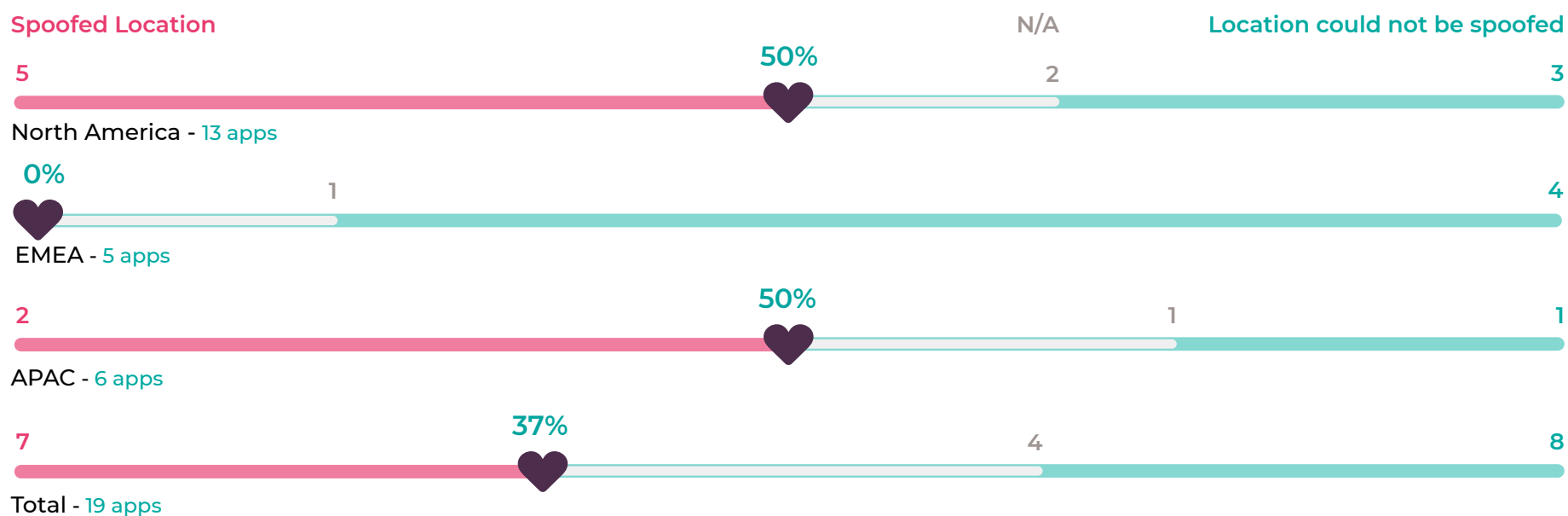
The initial check was to see if the app requested the user to share their real-time location.

The study results show that a high percentage of apps request the user to share their real-time location



## Location Spoofed, Location Spoofing Detected, N/A

For each app we checked whether when using a GPS spoofing app if the dating app displayed the real location of the user or the spoofed location. 50% of the apps in North America and in APAC displayed the spoofed location indicating that they were not detecting that the user's location was spoofed

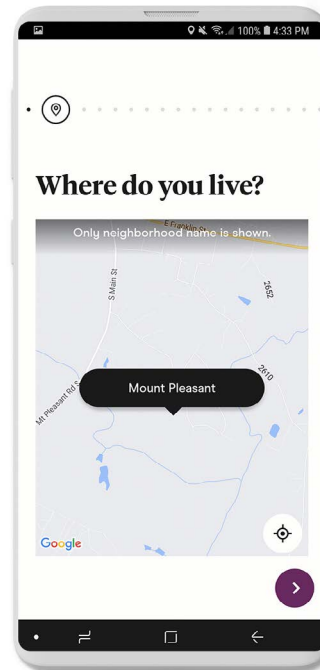


\*The 19 apps where location spoofing was attempted were the only ones which requested users to share the device's location

## Display of location information

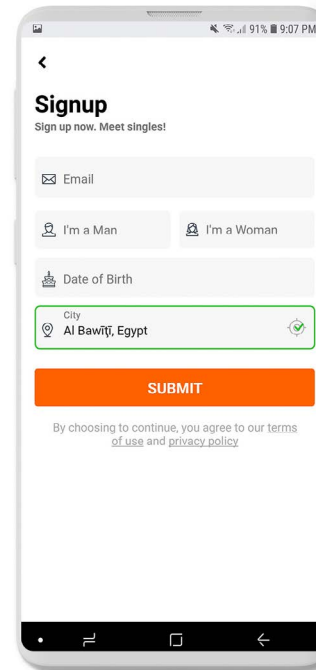
The manner in which the apps displayed the user's location varied. Some apps showed the user location during the onboarding process, other apps only showed the user location in the account settings screen or in the user personal profile.

The precision level and graphic presentation of the user location also varied: While some apps showed detailed location information in a map, others presented only the zip code, or even only city and country. In all examples, the user GPS location was used to determine the location displayed even if not in a map.



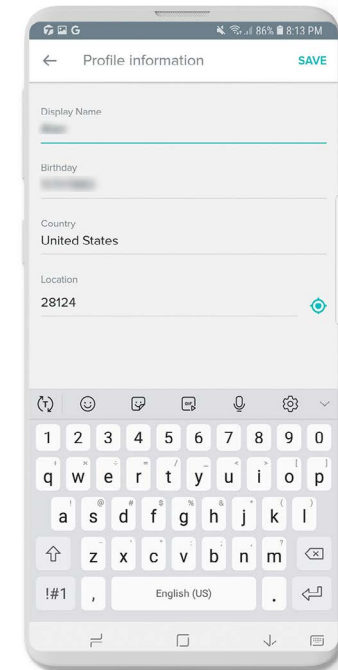
### Map

Example of user location being presented as a point on a map during the onboarding process



### City and country

Example of user city and country being displayed during sign up.



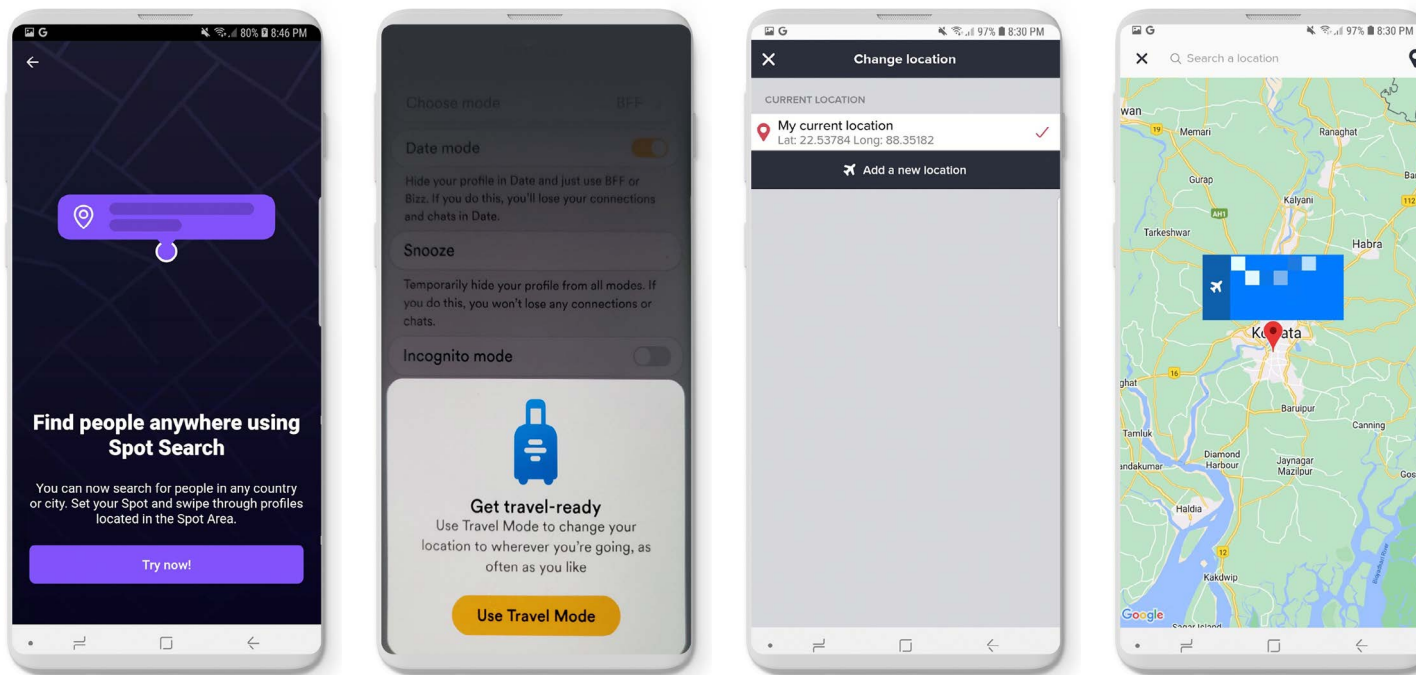
### Zip code

Example of user location being presented as a point on a map during the onboarding process



## Location Spoofing by design

Some apps presented the user with the option to change the location in which they would like the app to search for potential matches. Some displayed this purely as an option to change the location, others named the feature “Travel mode” or “Spot Research”. The ability to search for potential suitors in other locations, perhaps in anticipation of upcoming travel, is an interesting added feature. However, given the increasing level of catfishing and romance scams it would seem in the user’s best interest for trust and safety for the app to [leverage the users’ location to verify their real address](#) without interfering with the ability to search for suitors in other locations.



### Searching for Love in Multiple Locations

Examples of features allowing users to change the location they are searching for potential dating matches.

## A missed opportunity - location used for fraud detection

Given that all but one of the tested apps requested the user to share location data, location-based dating apps are now the norm. However, the implementation of requesting permission from the user to make use of their location data seems a missed opportunity.

**63% of apps which asked users for location permission did not present users with messaging on the benefit they would have by sharing their device's location.** In addition, 12 of 19 apps (63%) presented only the Android default screen when asking for the user to share their device's location, or did not explain why the app needed the device location. Only 7 out of 24 apps (<30%) presented custom messaging when requesting users to share their location. 0 of 24 apps (0%) informed the user that the app would use their location data to protect their account for security and fraud prevention - including prevention of catfishing and romance scams

### Location Messaging (% apps)

63%

Use default Android Messaging



29%

Custom messaging



63%

No messaging about benefits



0%

Messaging regarding trust & safety



No app informed the user that the app would use their location data to protect their account for security and fraud prevention - including prevention of catfishing and romance scams

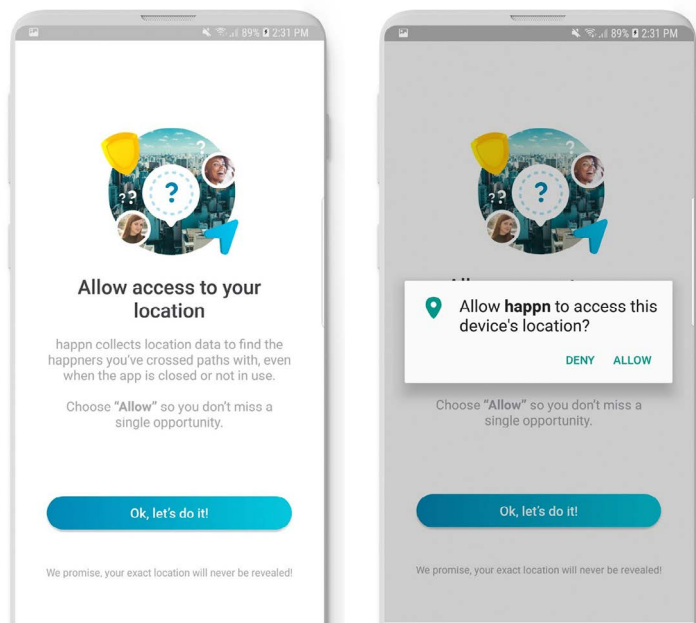
## Why provide a clear reason to request location?

Data from Incognia shows that providing a **clear reason for requesting location permission from a user that explains the benefits can increase location permissions opt-in rate to over 80%.**

Although some apps presented a clear reason for users to share their location, it was always focused on finding people nearby, not on account security. This is hardly surprising given that the #1 benefit to users for sharing their location on a dating app is to find potential suitors nearby. Since location intelligence can also be leveraged for verifying users address and providing highly accurate risk assessments it is a missed opportunity not to leverage a user's location for fraud and romance scam prevention.

Screenshots illustrating how different apps display the location (real or spoofed) of the user are included in the Appendix of this report. These screens were used to verify if the app considered the user at a real or spoofed location.

Clear reason for requesting location permission from a user can increase opt-in rate to over 80%.



### Custom Location Messaging Screen

Example of custom messaging screen requesting the user to share their location, explaining the benefit to the user.

## Summary

The results of this study show that location-based dating apps are now the norm with more than 90% of apps tested requesting the user's location to find potential suitors. At the same time **this study has shown that dating apps are susceptible to location spoofing, creating a trust and safety issue for users.** Using a free GPS spoofing app it was easy to demonstrate that 50% of tested apps in North America and APAC are not detecting and blocking basic GPS spoofing. Given the dramatic increase in 2021 in fraud losses from romance scams, and widespread catfishing, dating apps need to shore up their detection of fake suitors. **Increasing detection of location spoofing is an important step in safeguarding users on dating apps for increased user trust and safety and to prevent brand and reputation damage.**

### Learn more

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

[View resources](#) →

#### Ebook

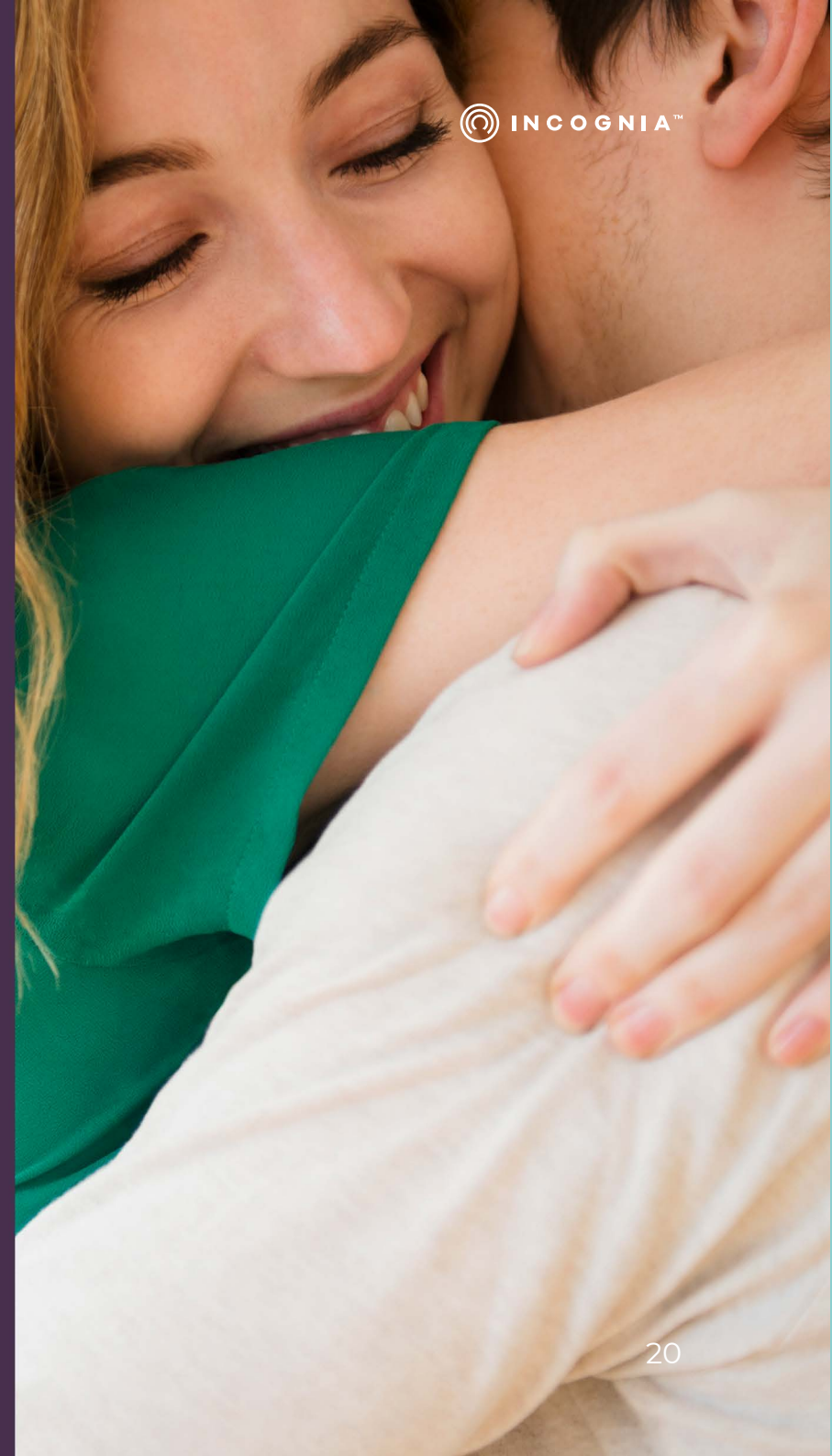
5 Ways Fraudsters Spoof Location

[Read now](#) →

#### Solution Brief

Location Spoofing Detection

[Read now](#) →



## About Incognia

Incognia is a privacy-first location identity company that provides frictionless mobile authentication 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 and is highly effective at detecting location spoofing. Deployed in over 200 million devices, Incognia delivers a highly precise risk signal with extremely low false-positive rates.



© 2022 Incognia All Rights Reserved