IDfy

The Ultimate Guide To

Keeping Fraudsters Away From Your Financial Platform

Today, financial companies around the world are posed with the challenge of providing complete safety to their customers by conducting secure transactions and maintaining the privacy of their databases. Studies show that in the United States of America, 4.8 million identity theft and fraud reports were filed with the Federal Trade Commission in 2020.

Fraud is defined as the intentional false representation or concealment of a material fact for the purpose of inducing another to act upon it to his or her injury. Fraud is always a scary scenario, not only in terms of the loss of money but also the loss of trust. People suffer from cases of stolen passwords, hacked bank accounts, identity theft, fraudulent transactions and more on a daily basis.

47%

of companies experienced a fraud in the past 24 months

3 Million

Fraud cases in USA alone

$42 Billion

is the total fraud losses reported by respondents

How To Checkmate Fraudsters

The best way to avoid fraud is identity verification where users are required to verify their identity in a secure manner, even before they enter your platform. Identity Verification during onboarding results in only authenticated users having access to the platform and keeps fraudsters at bay. But to learn more about identity verification, we must first explore the different ways in which one user can commit fraud on the platform.

3 most common ways fraudsters enter your system

There are many risks that you are exposed to if you don't identify the fraudster and allow them to sign up on your platform which can harm your business in multiple ways. There are three ways in which fraudsters can gain access to your system -

1 Fake Accounts

In this case, new accounts are created with the sole purpose of committing fraud. The fraudster pretends to be a legitimate customer by using fake identities. Some common warning signals would be

Recent IDs :
The government-issued ID is less than 60 days old.

Mismatched Information :
The applicant provided a different address than the address mentioned on their identification.

Tampered Documents:
The documents provided can seem unauthentic or might be tampered with.

2 Synthetic Fraud

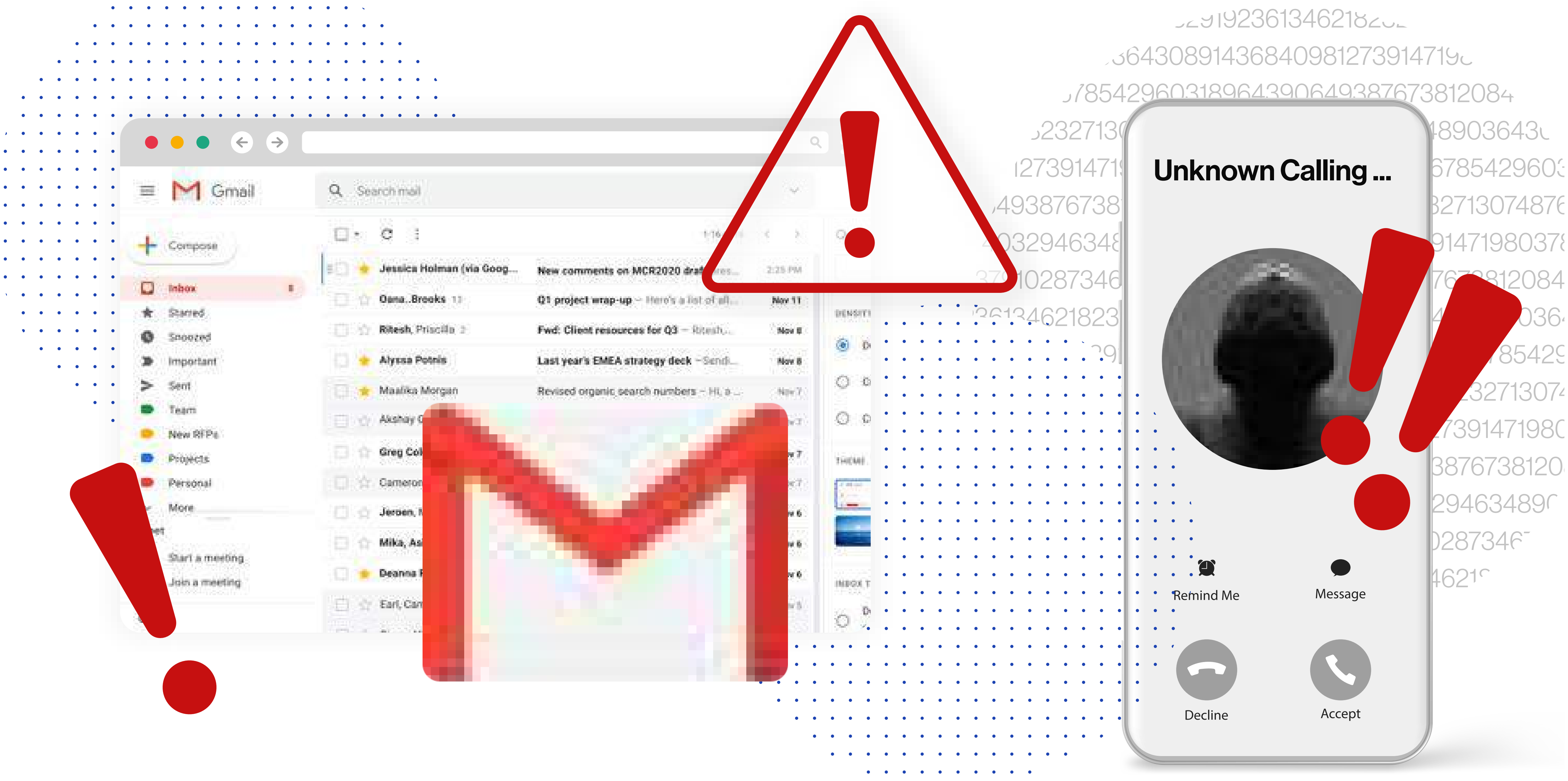
Synthetic identity refers to when they use multiple elements of information from different people to create a new identity, which is more difficult to detect as compared to stolen identities. It's the most sophisticated form of identity theft where fraudsters carefully hoard a cache of stolen bank account data, credit and debit card information, and other details to impersonate legitimate customers. Because fraudsters can take years to build good credit using a fake profile before making final fraudulent charges and abandoning the identity, it's one of the most difficult types of fraud to track down and catch.

3 Account Takeover

Here, cybercriminals gain access to the login credentials of a genuine account, allowing them to tamper with information and funds. Phishing, malware and other methods are ways to conduct account takeover and dupe people. Most of the time, it leads to fraudulent and unauthorised transactions.

Exposing their tricks
How do fraudsters do it?

By now, you are well-versed with the fraudulent activities that can occur. However, the process of how these activities go about is not common knowledge. Little is known about how people manage to hack into the system and commit fraud. We've conducted in-depth research and gained information about all the tricks up the sleeves of these fraudsters. Here's a quick run-through of ways in which they can bypass the verification process.



Fake Emails

How it works

Platforms request users for an email address and fraudsters turn to temporary emails for assistance. While the address appears to be authentic, they are typically only valid for a brief period.

The Risks

These temporary emails provide a temporary online mailbox for fraudsters to send and receive emails. They can easily verify themselves in the given time by accepting the activation links.

What to watch out or how to avoid

A simple method to screen out these kinds of frauds would be to verify the age of the email address. Checking if the email has been associated with fraudulent or suspicious activities in the past is another way to weed them out. Once you check these details, you're good to go!

Fake Mobile Numbers

How it works

This method works in the same way as email fraud, wherein fraudsters use a random mobile number provided by various websites to complete the verification process.

The Risks

The fake mobile number gives access to the user to a message box where they can receive text messages, allowing them to verify their identity.

What to watch out or how to avoid

A possible solution to identify whether a mobile number is fake is to check the age of the mobile number, as well as checking the previous activities conducted through the number.

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc
CĂN CƯỚC CÔNG DÂN
Số:
FAKE

ID Card Fraud

How it works

It is assumed that electronic ID cards are authentic and accurate. But fraudsters can easily tamper with the documents by using editing softwares like Photoshop. They can change the name, address, photograph, date of birth or any other information. People can also simply upload a picture of an existing ID card or use a paper over the ID card while clicking a picture.

The Risks

If the fake ID cards are not detected on time, they can allow the fraudsters to commit crimes and create colossal losses. Fake ID cards can amount to identity theft.

What to watch out or how to avoid

Review the ID cards provided by checking for low quality images, analysing the date of issue and other inconsistencies in structure or information. These red flags indicate possible tampering.

Document Fraud

How it works

Like in the case of ID Cards, fraudsters can tamper or forge non-standard documents such as bills, certificates, business licences, rental agreements, bank statements and many more using editing softwares. When it comes to merchant onboarding, fraudsters can provide legitimate documents that are not tampered with, but belonging to others.

The Risks

Fake documents can lead to easy verification of the fraudsters, allowing them to commit fraud. It can also lead to leakage of sensitive information. Using the documents of others is equivalent to theft of valuable information.

What to watch out or how to avoid

Fake documents can be detected if you notice a structural inconsistency in the files shared. Reviewing metrics like invoice numbers, low quality images and transactions in the case of bills can help spot documents that have been tampered with. Cropping of files, using black & white copies or scanned images are possible red flags.

Selfie And Deepfake Fraud

How it works

To fool facial biometrics, there are two kinds of frauds that can take place: spoofing and bypassing. In case of spoofing, fraudsters use silicone masks, printed photographs of other people, or even life-size mannequins to get onboarded or hack into accounts. For KYC via video, Deep Fake technology is on the rise. There are many deep fake generators available online that help fraudsters face-swap easily.

The Risks

Such advanced fraudulent activities can lead to major losses for financial institutions as they are harder to detect. People can easily impersonate others and falsify information.

What to watch out or how to avoid

The liveness solution chosen should analyse parameters such as image depth, skin texture, blood flow and eye reflections. State-of-the-art data encryption systems should also be employed to withstand hacking invasions.

Location Fraud IP Spoofing

How it works

Fraudsters use hacking to deceive a system into accepting a false location. A common method of doing so is Internet Protocol (IP) Spoofing, which occurs when a hacker alters the address within the IP header to fool a system into believing that the information is coming from a specific location or source. Location can also be manipulated with the use of VPNs, which conceal your real location and display a different location in another part of the world.

The Risks

Once IP Spoofing begins, it's very difficult to stop it. Location fraud allows fraudsters to present an authentic identity which will be verified easily.

What to watch out or how to avoid

To avoid these cyberattacks, use filters that examine headers of IP packets, enhance verification by not letting connections stay open for long without quality control. You can also use digital signing as well as IP encryption to keep hackers at bay.

How can IDfy help?

Capture

Any Document Accept

Capture data from any standard document from any country and non-standard documents from over 95+ countries.

Assited Video journey

Help users complete their pending onboarding journeys with video-based assistance from a 200+ managed services team.

Self Video Journey

Video activity capture. You can choose the type & the order of the activities that the user will be performing. We currently support activities like “Read random digits” and “Read the static text”.

Validate

Document Image Validation

Validate data such as names, ages, address from documents in any language, Check for document tampering or forging, Provide options to reupload in the same onboarding journey.

Selfie Validation

The platform validates the face on the id and the image captured. It's capable of detecting a 2D photo, multiple faces or faces outside of the frame in the selfie. Notifies in real-time and doesn't let the user upload. Liveness Checks to check if the person is trying to impersonate someone using some external means.

Extract

Extract Any Datapoint from Any Document

Extract data in any language from 95+ countries from standard documents like passport, license etc or non-standard documents like a utility bill, invoice, bank statements etc

Extract Any Rich Datapoint from Any Document

Extract facial pictures, signatures and more.

Authenticate

Email Validation

Prevent usage of email IDs that are associated with fraud during sign-ups

Mobile Number Verification

Prevent usage of fake numbers

IP Spoofing Checks

Check for any active VPNs set by the users to hide their current location. Good for location bound platforms

Selfie-based Identity Verification

Use Selfie to match the identity of the user with the documents uploaded

Liveness Check

Liveness and Face Match API to ensure a selfie is a real person.

Real-Time Location Identification

Verify location by capturing exact Lat-Long that ensures that the location isn't hidden by VPN, Validate the coordinates with the address on the documents, Prevent IP spoofing in any case.

Verify

Standard Checks

Deep verification against government databases with extensive checks against Credit Bureaus and alternate data sources

Alternate Checks

User information undergoes checks against international telecom. insurance and data acquired by other regulatory companies if standard checks aren't sufficient in a region

International AML Compliance

Ensure AML compliance across the globe by checking against 10000+ databases in real-time for Sanction lists, Warning lists, PEP checks, Adverse Media

Deliver Insights

Customized Journeys deliver insights

Monitor journey progress of each user, Analytics dashboard that keeps track of all processes in real-time, Customized real-time reporting

Report Categorization

Report on business performance, tech and product performance.

What our clients say

Arvind Ronta

Product Head - India & South Asia, Visa

We are happy to partner with IDfy at a time when we are reimagining the future of the industry.

Raj Karkara

CMO, ZebPay

Using IDfy's identity verification solutions has enabled us to onboard users from multiple jurisdictions in a cost and time-efficient manner. Their document capture and selfie check APIs do a wonderful job by lowering the time taken to verify a user to just under 2 minutes.

Amit Kurseja

Head - Merchant Acceptance, Amazon Pay

IDfy plays a great role in innovations, making hit-and-try experiments possible, due to the platform's capability to quickly conduct KYC and verification of merchants.

MARKET LEADERS TRUST US

paynamics Your trusted online payment partner

PhonePe

VISA

Paytm

amazon pay

Fidelity INVESTMENTS

zebpay

hop Banking - Smarter, Faster, Better

kotak Kotak Mahindra Bank

IDFC FIRST Bank

MOTILAL OSWAL Asset Management

ETMONEY

Worldline

IDfy

Hey! We are IDfy.

We help fintech and finance companies onboard genuine users in 2 mins from over 95+ countries.

We block impersonators, fraudsters by detecting and preventing fraud at the source. While accurately identifying entities and verifying their credentials in return ensuring compliance needs.

We would like to learn about your challenges in this space. Connect with us at emily@idfy.com to know more about how our collaboration can prevent any incoming fraud on your platform.

Thank you for reading.

Unlock the Real