

VERIFF IDENTITY FRAUD REPORT

All the trends you need to stay ahead of bad actors, protect your customers, and safeguard the future of your business in 2023.



CONTENTS PAGE

■	INTRODUCTION	1
■	ROOTING OUT FRAUD ACROSS THE WORLD	2-4
■	FINANCIAL FRAUD: WHAT YOU NEED TO KNOW	5-7
■	CRYPTO FRAUD AT A GLANCE	8
■	THE PERSISTENCE OF PHISHING	9-16
■	ON THE FRONT LINE OF FRAUD PREVENTION	17-20
■	KEEPING YOUR BUSINESS AND CUSTOMERS SAFE	21-24
■	WHY INVESTING IN FRAUD PREVENTION IS A MUST FOR YOUR BUSINESS	25
■	OUR INNOVATIONS	26
■	OUR AUTHORS, CONTRIBUTORS, & SOURCES	27-28

INTRODUCTION

Fraudulent activity is increasing, and increasing fast — with our data revealing an 18% increase in fraudulent activity year-on-year from 2021 to 2022.

Fighting fraud is our business and understanding the global fraud landscape is vital to our goal of creating a safer online world for both businesses and individuals.

Our fraud report encompasses the big picture — how the world is reacting to global events like COVID-19 and the resulting economic downturns — and how fraud is impacting businesses worldwide. This year, however, we also focused on something plaguing both businesses and consumers alike, phishing.

This specialized type of online fraud — in which attackers attempt to trick users into harmful action (such as clicking a bad link that will download malware or direct them to a malicious website) — was identified as being a particular problem for our customers.

This report shares the insights our expert team has discovered on the front line of fighting fraud — giving you the tools to protect both your business and your customers.

* The data for this report was collected from Veriff's inhouse digital identity verification sessions during the period of January 1st, 2022 - November 1st, 2022.

ROOTING OUT FRAUD ACROSS THE WORLD



THE RISK OF FRAUD IS GROWING

17.90%

In 2022, Veriff saw a 17.90% increase in fraudulent activity compared to 2021

10TH

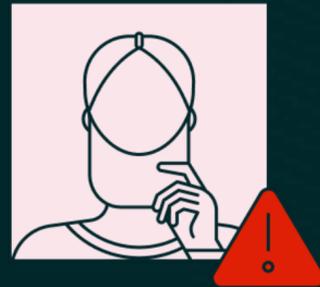
Close to every tenth verification Veriff has seen between January and October was fraudulent

51%

Over half of those were identity fraud

46.62%

The most significant growth has been in recurring fraud across industries, which has seen 46.62% increase YoY



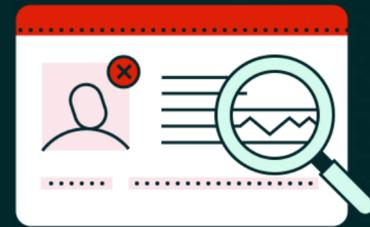
Recurring fraud on the rise

Over half (51%) of fraudulent activity worldwide is still identity fraud. However, in 2022 Veriff saw the biggest increase (46.62%) in recurring and pattern fraud, where criminals have been successful before and are trying to trick the system again — 43% of all fraudulent verifications are recurring. Second most significant growth was in document fraud, which grew by 33.13% globally.



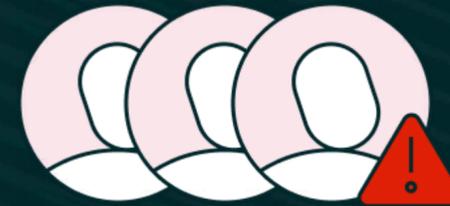
Disparities between targeted sectors

Across industries, 7.81% of verifications have been fraudulent in 2022; for crypto businesses the fraud rate has been 9.61% and for financial services providers 5.84%.



Fraudsters are on the move

In 2022 both the U.S. and Europe saw a significant jump in document fraud, which makes up the majority of fraud across industries. This year, fraudsters have moved outside Europe and the U.S. bringing more fraud to countries like Uzbekistan (28.12%), Kazakhstan (22.86%), Belarus (22.51%), Paraguay (21.94%), and Thailand (20.76%).

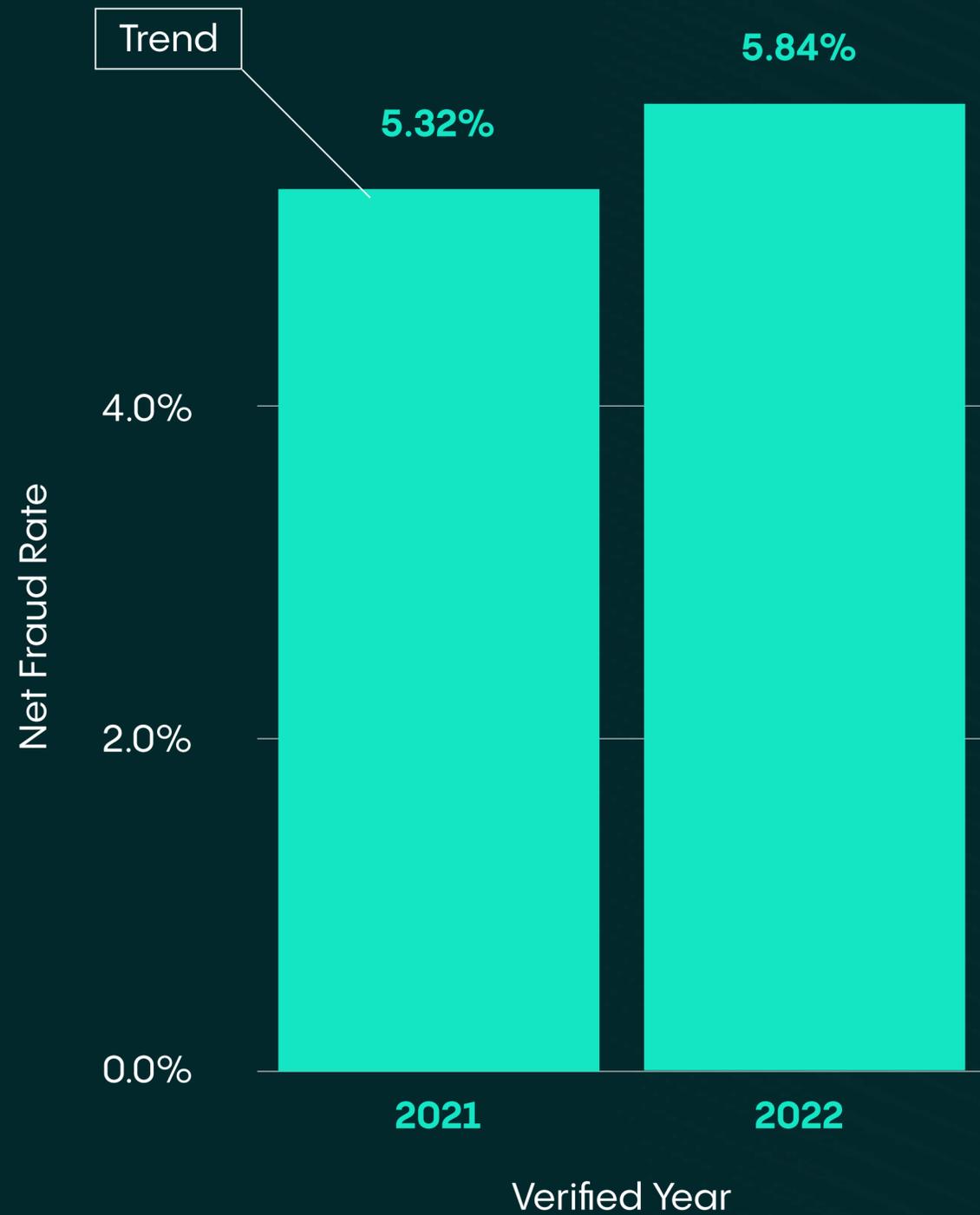


Fraud innovations: Identity farming

9% of all fraud is made up of identity farming, which is a type of online fraud in which an individual or group of individuals creates numerous accounts on a large scale to engage in various forms of fraud.

FINANCIAL FRAUD: WHAT YOU NEED TO KNOW

veriff 



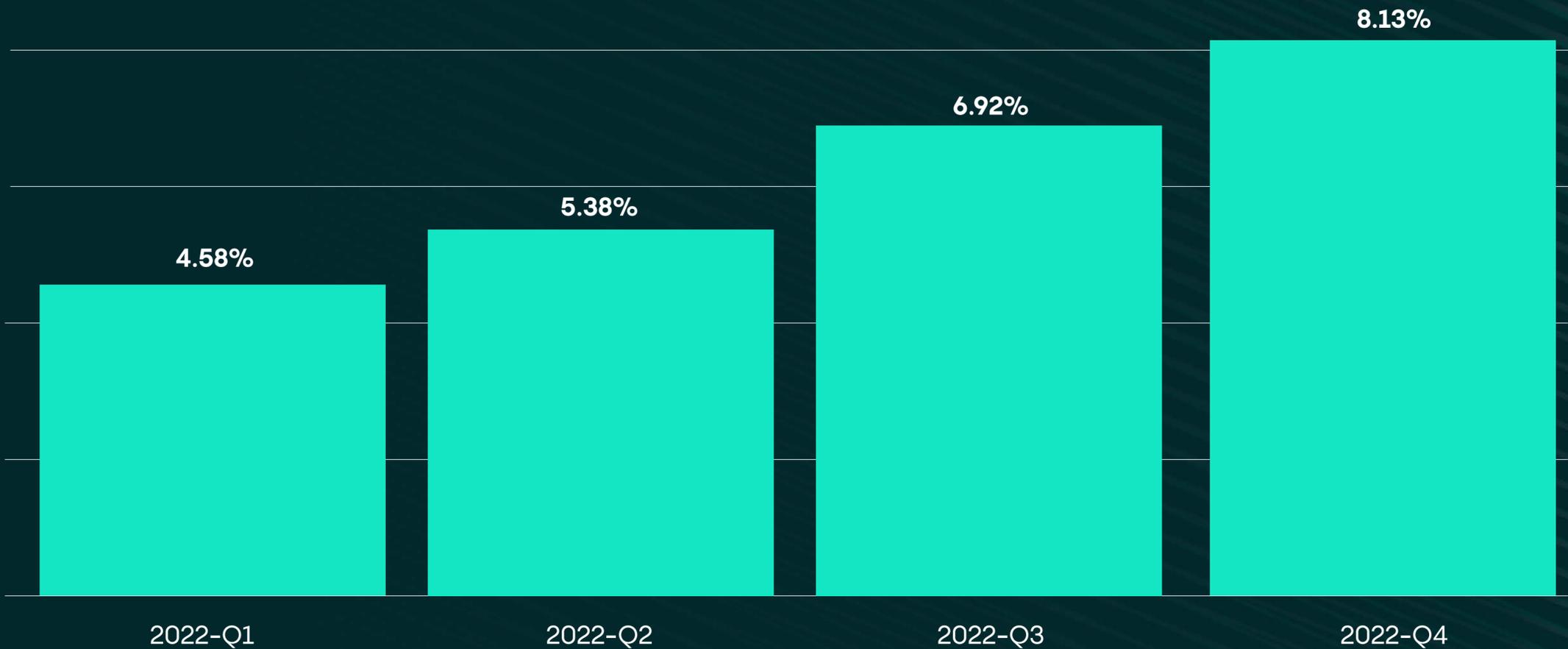
Graph 1. Net Fraud Rate

Businesses operating in the financial sector experienced 5.84% of fraud that Veriff saw in 2022. Financial services businesses have seen a significant increase of 79.02% in document fraud compared to last year.

Over half (51%) of all incidents in financial services fraud are made up of identity fraud.

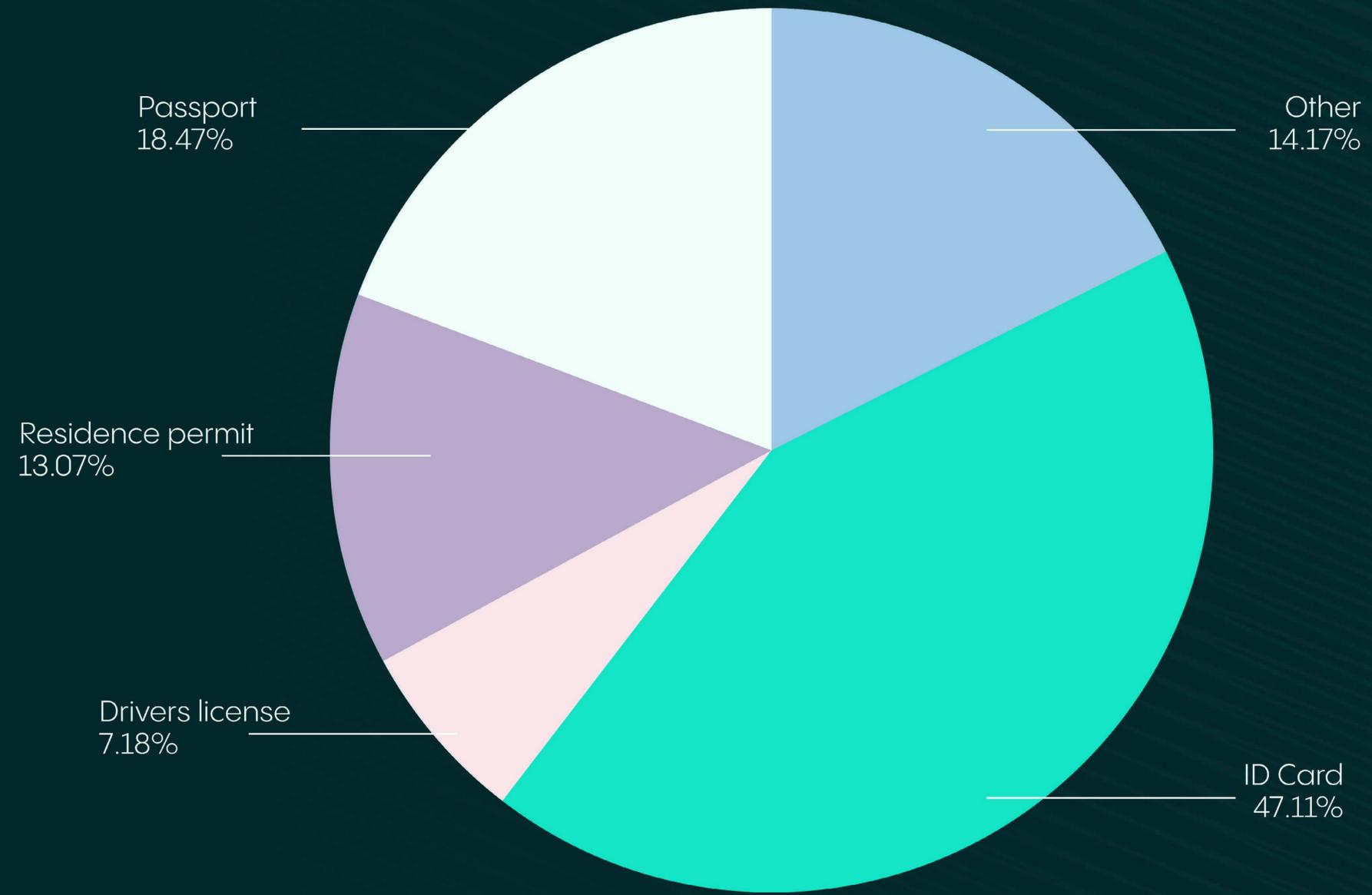
FINANCIAL SERVICES FRAUD RATES BY QUARTERS

- A STEADY RISE:



Graph 2. Increase in Financial Services Fraud Rate

TOP DOCUMENTS USED FOR FRAUD:



Graph 3. Top Document Types Used for Fraudulent Activity in Financial Services 2022

CRYPTO FRAUD AT A GLANCE



Cryptocurrencies are disrupting the world of finance. However, because cryptocurrencies are cryptographically secured on their blockchains, transactions between users are generally anonymous and take place in an instant. Due to this, crypto transactions provide opportunities for criminals who are looking to evade conventional Anti-Money Laundering controls.

Crypto businesses have seen a rapid increase in fraud in 2022 – 25.23% more than the year before. On average, close to every tenth (9.61%) verification Veriff has done has been fraudulent.

Types of fraud in crypto:

The most significant growth (81.70%) in crypto fraud came from document fraud where a person alters the information on ID documents or creates fake ones with the aim of defrauding the verification process. Document fraud makes up 43% of all fraudulent verifications Veriff saw in crypto in 2022. Identity fraud and recurring fraud have seen more than 10% growth each compared to 2021.



Graph 4. Growth of Fraud in Crypto

According to FBI statistics, cryptocurrency fraud that involved Bitcoin, Ethereum, Litecoin, or Ripple, totaled more than \$1.6 billion.

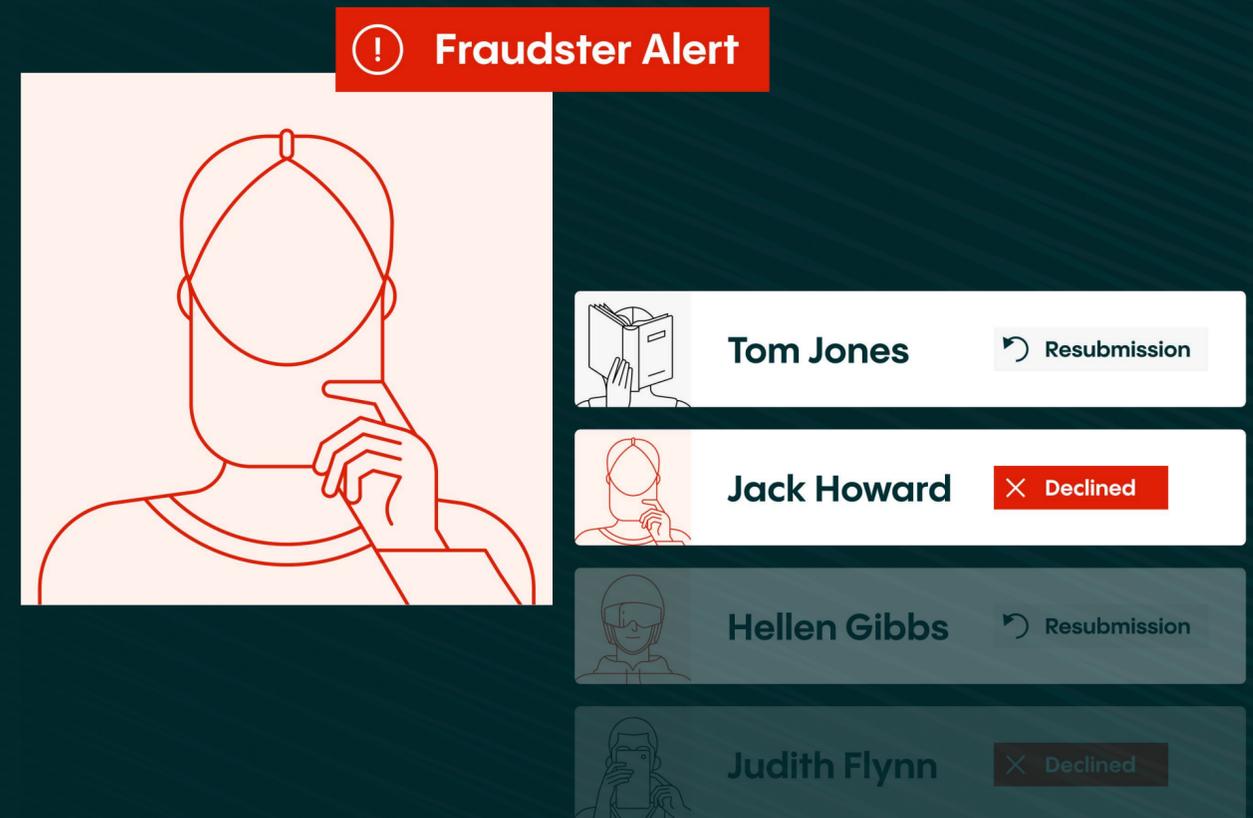
THE PERSISTENCE OF PHISHING



The first recorded use of “phishing” was used in 1996 on the beginnings of AOL. The early phishing attacks were mainly credit card scams, where hackers would steal victims passwords to then run an algorithm that randomized credit card numbers that were used to open other accounts and spam other users.

In 2017 fraudsters started adopting HTTPS and implementing web encryption to lure victims into a false sense of security. This makes it easier for hackers to get victims to enter credentials and personal information that they can use to gain access to several financial institutions.

This year was also the year that ‘conversation hijacking’ became popular among fraudsters, which is “a style of phishing email in which hackers insert themselves into email conversations between parties known to and trusted by one another.”



In the next few years the types of scams that became prevalent were vishing scams, which are voicemail scams, and fraudsters preyed on the widespread familiarity with business voicemail. Additionally, according to Microsoft, scammers are now distributing emails with fake Google search results that lead to attacker-controlled websites.

While it's been more than 25 years since the term was coined, the world hasn't found a way to eliminate internet scamming — in fact the process has become more advanced, and more dangerous for both consumers and businesses.

According to the FBI 2021 Internet Crime Report, between 2017 and 2021, over \$18 billion was lost due to internet scams, and in those five years the phishing complaints went from 25,344 to over 323,000.

In the recent past, COVID-19 necessitated lockdowns and social distancing requirements that have fast-tracked the transition of many essential governmental and highly regulated non-governmental services to the digital medium.

This means, that more than ever before, people are using the internet to carry out tasks that require them to share sensitive, personally-identifiable information across multiple platforms.

Though governments worldwide have been working tirelessly to draft stricter and more holistic data protection policy (DPP) laws, cases of data theft have still been on the rise. On an organizational level, data theft is carried out in two main ways, read about these on the right hand side.

Though data theft from organizations causes a loss on a larger scale, fraudsters are equally active when it comes to targeting individuals, especially the ones that have not been exposed to the world of the internet for too long, to steal or collect identity-related information.

One of the most prevalent ways in which fraudsters target individuals is through Social Engineering. Social Engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.

DATA BREACHES:

A data breach is a security violation in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Such incidents can result from coordinated and deliberate attacks by highly skilled individuals or groups who target various governmental or private institutions.

DATA LEAKS:

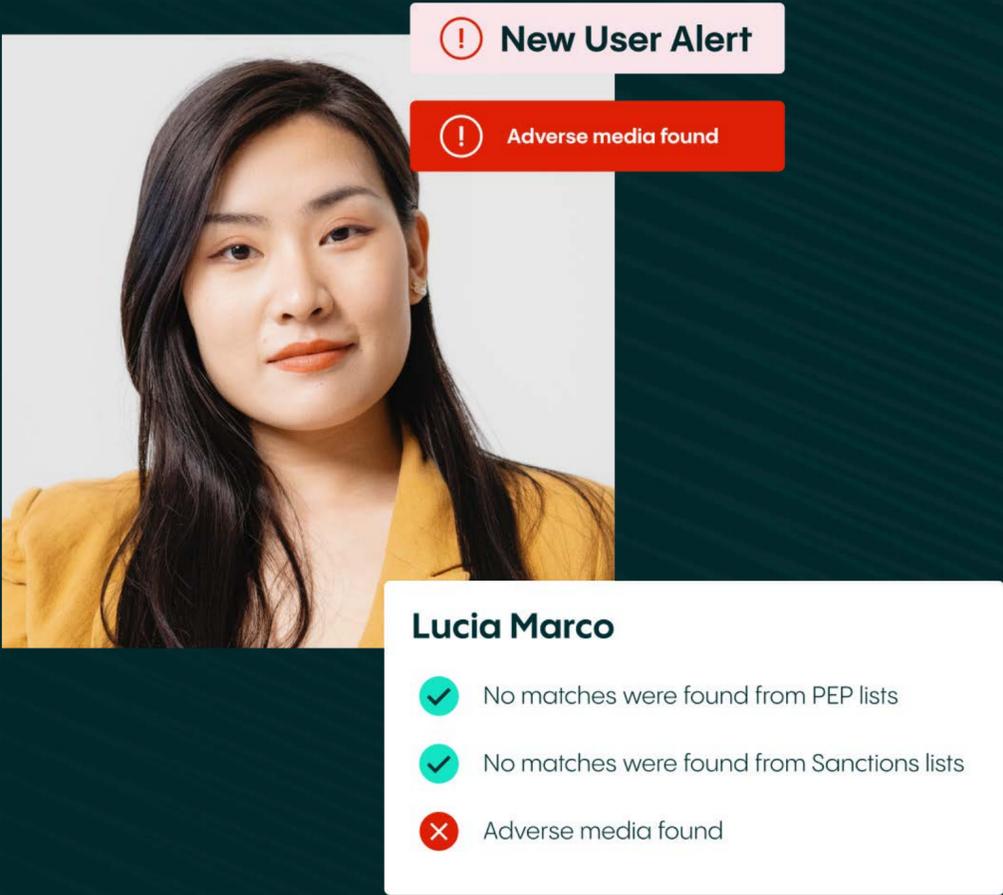
There is a small but key difference between a Data Breach and a Data Leak. In Data Breaches there is a conscious attempt by a third party to infiltrate and access data, and in Data Leaks the unauthorized loss of data happens simply because of poorly configured system security or careless disposal of used computer equipment or data storage media.

VARIATIONS OF PHISHING 2022

There are several types of phishing attacks that Veriff documents, so we've broken down the most popular types of phishing and how attackers utilize them to scam victims.

Phishing is a technique for attempting to acquire sensitive data — such as bank account numbers — through fraudulent solicitation in emails or through a website, in which the perpetrator masquerades as a legitimate business or person.

Though there are many different established techniques, fraudsters are evolving and using newer techniques to perpetrate different phishing scams, some of the most well-known and widely used techniques are as follows:



The image displays a user verification interface. On the left is a portrait of a woman with long dark hair wearing a yellow jacket. To the right of the portrait are two notification banners: a pink one with a red exclamation mark icon and the text 'New User Alert', and a red one with a white exclamation mark icon and the text 'Adverse media found'. Below these is a white verification status panel for 'Lucia Marco' containing three items: a green checkmark icon with the text 'No matches were found from PEP lists', another green checkmark icon with the text 'No matches were found from Sanctions lists', and a red 'X' icon with the text 'Adverse media found'.

VISHING

Vishing is a Phishing scam that happens over phone calls (most often using Voice over Internet Protocol). In a Vishing scam, a fraudster will contact a potential victim by phone (using a VoIP account) impersonating either a person within the victim's circle of trust or technical support staff from one of the victim's banks or service providers.

Often, the fraudsters will already have collected some personal information on their victims—such as bank information, account numbers, or even credit card numbers. This allows the fraudsters to lull the victims into a false sense of security and cause maximum financial damage.

SMISHING

Smishing or SMS phishing, is the act of committing text message fraud to lure victims into revealing account information or installing malware. Like phishing, cybercriminals use smishing to attempt to steal credit card details

or other sensitive information by disguising themselves as a trustworthy organization or reputable person in a text message.

PHARMING

Pharming is when a fraudster uses a virus or similar technique to hijack the victim's browser without their knowledge. The primary objective of the virus is to redirect the user to an identical mirror website created by the fraudster that replicates a website for the victim's bank or other financial institution.

This website is then used by the fraudster to collect critical information, such as bank IDs and passwords or credit card numbers, which the victim unknowingly submits without even realizing they aren't on the reputable site.

BUSINESS EMAIL COMPROMISE

Business email compromise (BEC), also known as email account compromise, is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct personal and professional business.

In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request.

ON THE FRONT LINE OF FRAUD PREVENTION

veriff 

Our expert fraud team is not only fighting fraud, but documenting how fraudsters are trying to infiltrate our systems so that we know how to combat repeat attacks and any copycat scammers. We've pulled a selection of the group fraud and coordinated attacks that Veriff's fraud team has seen to showcase the full array of tactics that phishers are using in 2022.

DEEPFAKES

A group of scammers were exclusively using sophisticated deepfakes to recreate passports to make them seem more lifelike. Veriff was able to ascertain that the group was using the same set of devices to create sessions with the deepfakes.

The amount of sessions and overall traffic from this one group grew to the point that it was 90% of the traffic for the specific passport specimens they were using. Over 200 sessions were detected from this group and all of the sessions were caught and declined by Veriff automation.



! Fraudster Alert



TRUE LOVE SCAM

In romance scams, fraudsters usually create fake online profiles with fictional identities, pictures, and names to lure their victims into transferring them money or property. After the contact is established, they start expressing strong emotions and sharing 'personal' information with their victim.

After gaining their victims' trust, they ask for money for some sort of 'personal emergency' and these scams usually end in big financial losses. Veriff has observed similar accounts – including a victim being lured into opening a Blockchain account in the U.S.

The scammer was caught when verifying details with Veriff's liveness detection after asking the victim to send additional pictures of themselves for authorization.

Romance scams are evolving just like other types of fraud. According to FBI data, in 2021 there were close to \$1 billion in losses due to romance scams – this accounted for the third highest losses reported by victims.

Additionally, more and more victims of romance scams that are reported are linked to investing in cryptocurrency opportunities. In 2021 there were over \$429 million in losses due to cryptocurrency specific romance scams.

FAKE JOB AD

A group of fraudsters put a fake job ad on Facebook claiming to represent a South American company. Over 100 users applied for the job, and after scammers collected their CVs they opened Blockchain accounts on their behalf. When identity verification for a wallet was required, fraudsters sent 'magic' links to the victims as part of the 'hiring process.'

One of the victims contacted Veriff's customer support to verify whether we offer services for the company, and they also contacted the company for whom they allegedly did the verification, and found out that online identity verification was not part of the company's hiring process.

Veriff reviewed the sessions and the scammers had made it appear as if the end-users were applying for a job instead of creating a crypto wallet.

Using Veriff's background video detection, our fraud team was able to detect similarities between all of the sessions that were submitted for the "job application" and were able to detect similar advanced fraud rings.

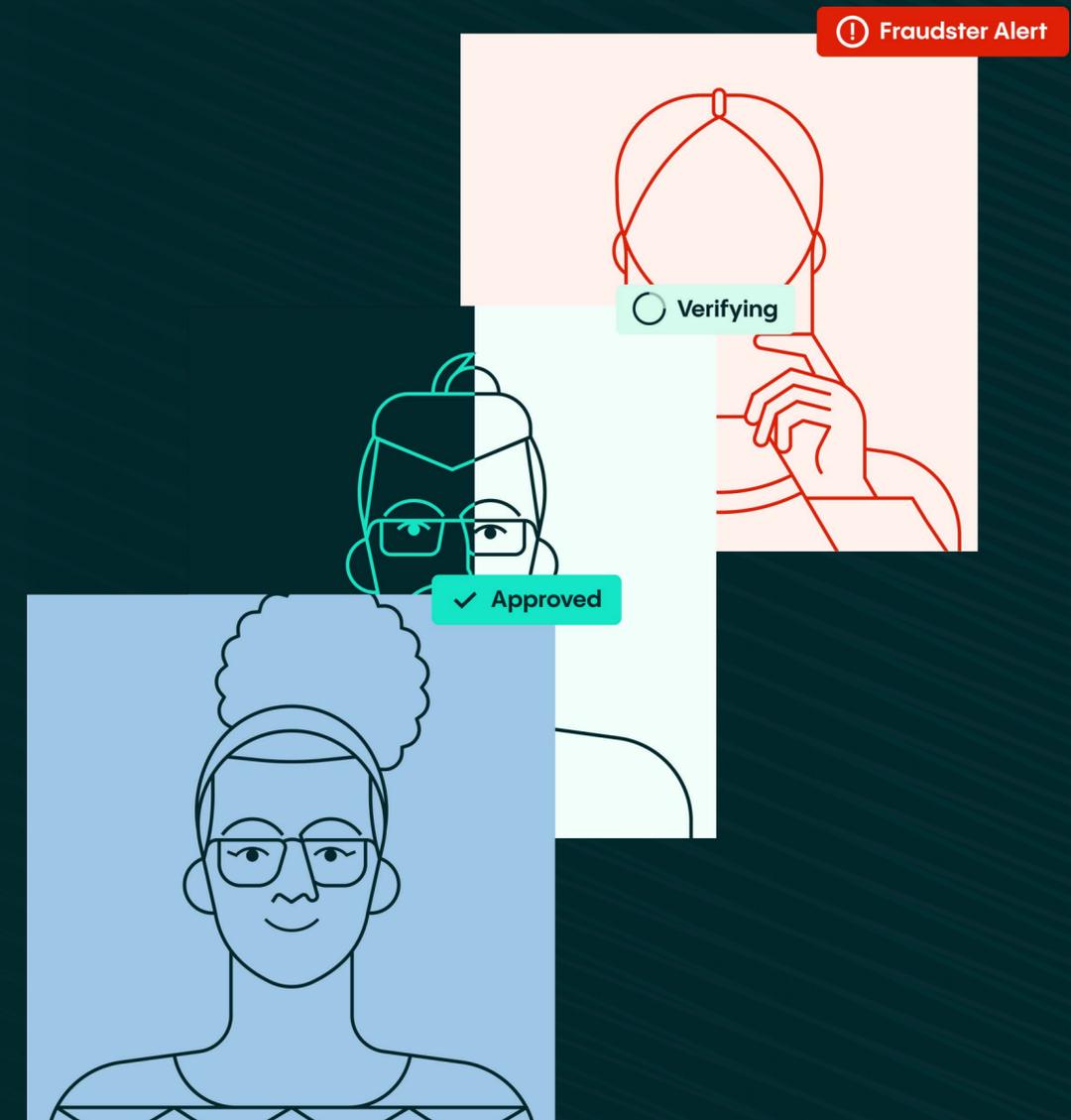
**KEEPING YOUR BUSINESS
AND CUSTOMERS SAFE**

veriff 

Phishing's constant presence has enumerated the many problems with consumer's understanding of how financial institutions work, but it also represents a large gap in the identity verification space.

As traditional banking updates to allow for more online transactions, and neobanks and crypto continue to boom, the need for well-rounded and comprehensive identity verification has never been more important.

Veriff tackles fraud from multiple angles to ensure that we are not only catching fraudsters at the moment, but implementing safeguards against recurring attacks and organized fraud rings.



HOW VERIFF IS STOPPING FRAUD

✔ An end-user flow that is intuitive, and has built-in features that promote increased safety without slowing down the process such as:

- ✔ Liveness detection
- ✔ Biometric analysis
- ✔ Real-time user feedback

✔ A full-stack AML and KYC solution

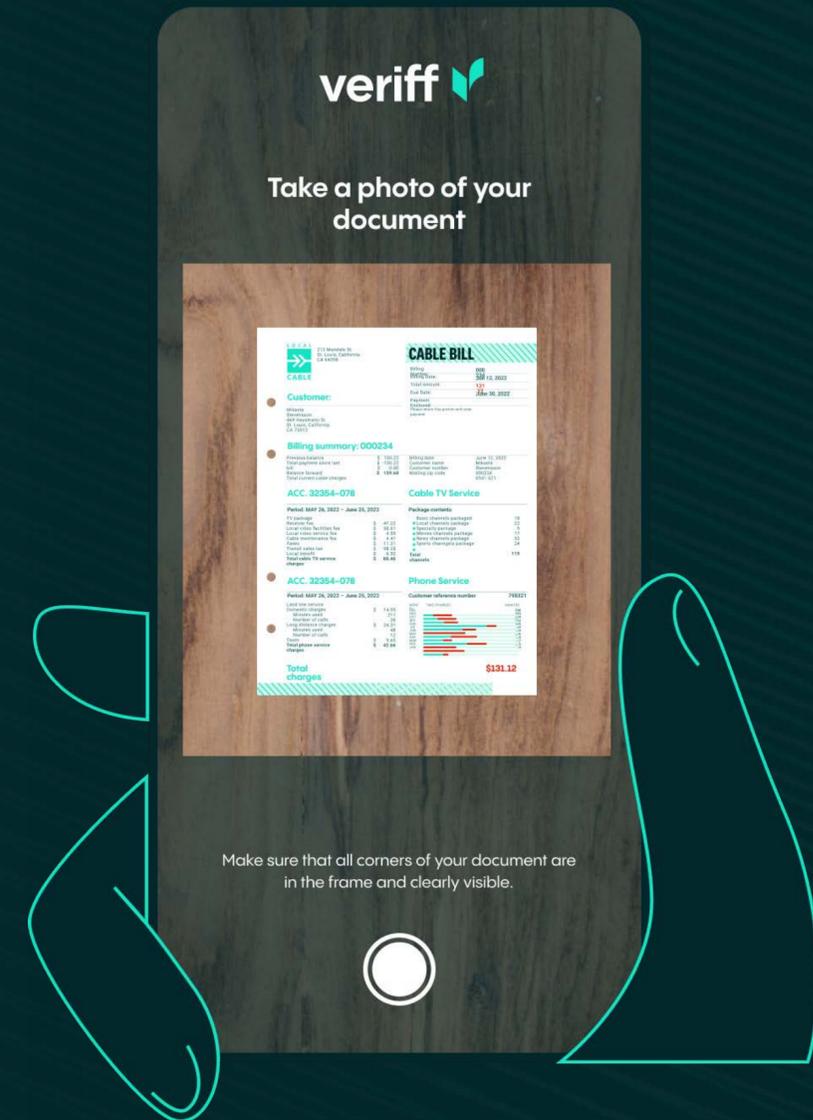
✔ The largest language and identity document database on the market

✔ Biometric Authentication, which negates the need for legacy 2-factor authentication

The key elements of our fraud prevention engine are the device and network fingerprinting solution and crosslinking. Crosslinking allows Veriff to group together sessions that share similar data points.

For example, sessions submitted by the same person, on the same network, with the same device and/or using the same document. We also check for velocity/abuse to ensure that no end user compromises a service via multi-accounting.

All of this information we see through crosslinks and we can automatically discard users if they, their document or their device has been approved before. Crosslinking has been imperative in stopping phishing and identity farming because it allows Veriff to detect patterns that often emerge when analyzing phishing scams.



VERIFF USES A VARIETY OF TECHNOLOGIES AND STRATEGIES TO CATCH PHISHING, INCLUDING:

In-house device and network fingerprinting service derived data points to analyze traffic quality.

Fraud Risk Labels used by our specialists analyze the various aspects of the incoming traffic and their link to any of the known fraudulent sessions.

They provide insight about the final decision and help in post-verification analysis.

In-house developed business intelligence solutions to continuously monitor all possible areas of threats or exploits.

For specific clients, Veriff also uses machine-learning based risk identification to pay more attention to sessions that are classified highly risky based on our experience and client-approved methods.

Veriff allows its clients to use a "Blocklist" that allows us to block known fraudsters based on their facial features.

WHY INVESTING IN FRAUD PREVENTION IS A MUST FOR YOUR BUSINESS

veriff 

Forrester Consulting conducted a commissioned Total Economic Impact™ (TEI) study on behalf of Veriff on the potential benefits of deploying Veriff's Identity Verification Platform, and the results had information regarding the return on investment in comprehensive identity verification with Veriff. The enterprise that Forrester interviewed was an investment platform with an annual revenue of \$1.5 billion in year 1.

The study found that Veriff **enabled the organization to cross-link customer verification sessions with past customer identification activity, matched fraudulent behavior to a device fingerprint which significantly reduced the chances of recurring and organized fraud, and standardized the process of authentication making it more dependable.**

*Results were based on an interviewee's organization

The results of the Forrester study were significant and showed a 195% return on investment in Veriff's platform over three years. In addition to the ROI, there was a 20% reduction in fraud risk, and on average 8 minutes saved on each identity verification session.

Veriff allowed for a greater level of compliance, while also providing a much better user experience which has proven to increase customer conversions significantly.

OUR INNOVATIONS

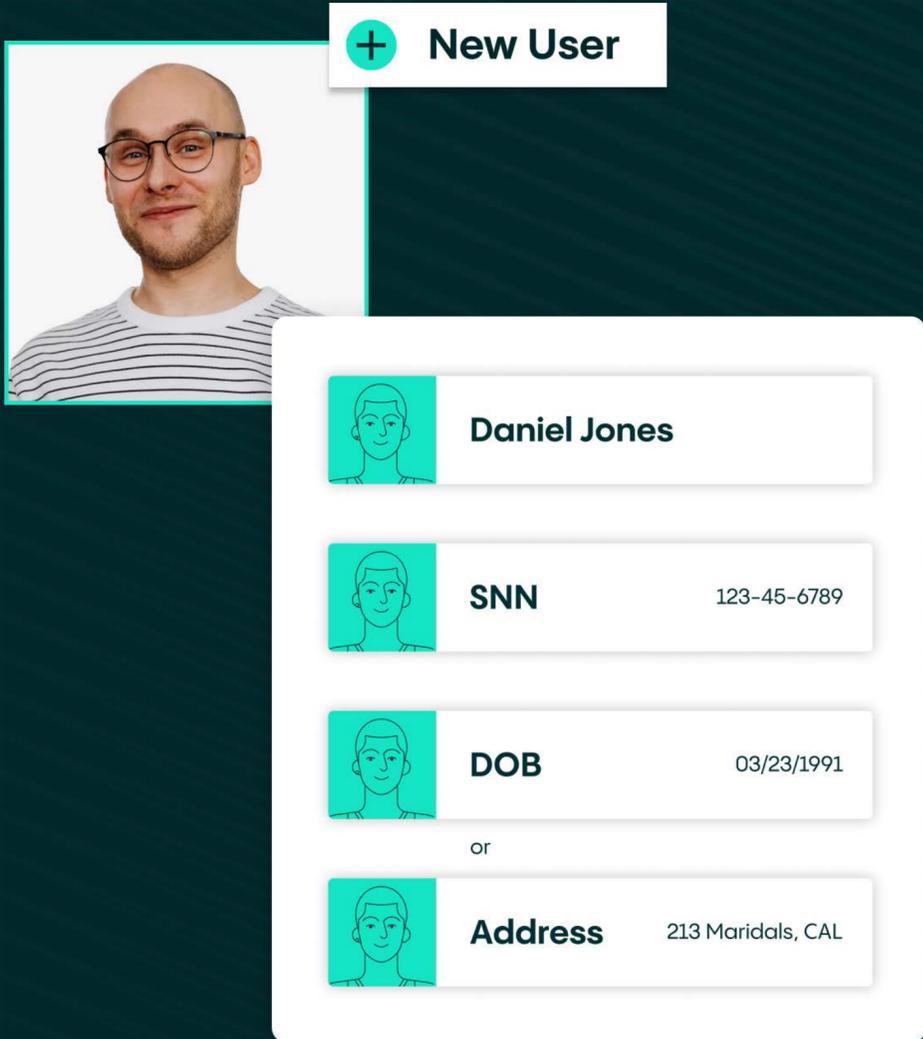
veriff 

To tackle fraud, Veriff's leading identity verification technology has only gotten stronger throughout 2022. With new products that work across thousands of use cases, Veriff's continued focus is to be the partner that keeps businesses and customers safe, while making the process easy and hassle free for all involved.

Veriff launched Proof of Address and Social Security Number verification, as well as unveiled our brand refresh that makes the Veriff mission undeniably clear: we want to make the internet a safer place.

LOOKING AHEAD

In the new year Veriff will be rolling out new functionality around our crosslinking technology, which will be an update to our fraud prevention capabilities. Our new technology will leverage businesses in the Veriff network to identify and block repeat fraudulent actors in specific industries. This product will be another tool in Veriff's arsenal to stop fraud in its tracks.



A user profile card for Daniel Jones. At the top left is a photo of a man with glasses and a beard. To the right of the photo is a button with a plus sign and the text "New User". Below the photo is a list of user details, each with a small profile icon on the left:

- Daniel Jones**
- SNN** 123-45-6789
- DOB** 03/23/1991
- or
- Address** 213 Maridals, CAL

AUTHORS, CONTRIBUTORS & SOURCES

OUR AUTHORS AND CONTRIBUTORS

Iryna Bondar Fraud Operations Team Lead

Iryna leads the Fraud Operations team, which consists of a combination of multiple fraud specialists, quality control specialists and fraud analysts.

As part of her broader responsibility, Iryna coordinates and assists various internal stakeholders in covering fraud-related blindspots by identifying vulnerabilities and putting into place fraud preventive measures using insights driven from multiple fraud vectors.

Munna Poddar Fraud Engineer

Munna helps identify key trends and relevant use cases within the wider fraud domain to help Veriff build data-driven and advanced analytics-backed Fraud Prevention solutions for existing and future clients.

Prior to joining Veriff, Munna was working with Microsoft's Human Intelligence team to find innovative and effective strategies to prevent fraud within Microsoft's Azure and MS Learn businesses.

Papuna Abesadze Data Analyst

Papuna is a Data Analyst in charge of defining and maintaining the logic behind our sophisticated Fraud Metrics.

He helps Veriff's Fraud division with large-scale analytics, data modeling, and BI tooling to make sure not even the most inconspicuous emerging trends escape our attention.

SOURCES:

2022 Identity Fraud Study: The Virtual Battleground

<https://javelinstrategy.com/2022-Identity-fraud-scams-report>

State and Tribal Child Welfare Information Systems, Information Security Data Breach Response Plans (PDF) (Report). United States Department of Health and Human Services, Administration for Children and Families. 1 July 2015. p. 2. ACYF-CB-IM-15-04. Archived (PDF) from the original on 11 November 2020.

<https://www.acf.hhs.gov/sites/default/files/documents/cb/im1504.pdf>

Social Engineering Definition

<https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering>

Phishing definition

<https://csrc.nist.gov/glossary/term/phishing>

What is Smishing?

<https://www.barracuda.com/glossary/smishing>

FBI Safety Resources – Business Email Compromise

<https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise#:~:text=How%20to%20Report,office%20to%20report%20the%20crime>

The Quiet Evolution of Phishing

<https://www.microsoft.com/en-us/security/blog/2019/12/11/the-quiet-evolution-of-phishing/>

The Total Economic Impact™ Of The Veriff Identity Verification Platform a commissioned study conducted by Forrester Consulting on behalf of Veriff, March 2022

FORRESTER®

CONTACT US!

If you'd like to learn more about Veriff's fraud prevention, you can visit our website or contact us via sales@veriff.com

veriff.com

