IDnow.

Trend Report: Identity Fraud 2021.

How to win the cyber fraud arms race.

Cybercrime is undergoing an industrialization wave and booming like never before, it is a massive business in its own right. Cyber fraud already is one of the biggest threats to our economy. The latest predictions say the damage caused by internet fraud will amount to $6 trillion in 2021. The global Covid-19 pandemic accelerated digital transformation massively in every industry – but unfortunately, this was accompanied by a drastic increase in fraud.

The need for user-friendly and fast digital processes is greater than ever. Not only have customer expectations changed over the last few years – users expect services to be available within minutes, not days – but the current situation has also forced many companies to act and adapt quickly.

Unfortunately, crime never sleeps, and IDnow has noticed in 2020 a significant increase in fraud attempts since the first lockdown. In this Trend Report, we want to give you an overview of the cyber fraud landscape – read on and find out how we are working hard to remain one step ahead of criminal minds all over the world.

Fraud on the rise.

One challenge of living in a digital world is often not knowing with whom you are interacting – and that is absolutely critical when doing business. Static identifiers such as passwords and email are not always reliable because they can be stolen.

So, to know who you are interacting with, strong authentication is crucial. In general, B2B authentication prioritises security while business to consumer authentication focuses on simplicity. In recent years, many countries have introduced strict Know Your Customer (KYC) requirements for account opening and online transactions to fight money laundering and terrorism funding.

Financial crime is a severe threat, estimated by the UN at $800 billion to $2 trillion worldwide per year. The European Union’s fifth Anti-Money Laundering Directive (AMLD 5) came into force on January 10th, 2020, with the aim of creating greater transparency to due diligence requirements and limiting anonymity in order to combat financial crime. The Directive also places greater emphasis on transparency around beneficial ownership in order to fight financial criminals who have hidden behind complex corporate structures.

Financial crime is estimated by the UN at

$800 billion to $2 trillion

worldwide per year.

70%

of decision-makers in German companies see online data fraud as the most significant cyber risk.

40%

increase in attempted cyberattacks within a week of the lockdown.

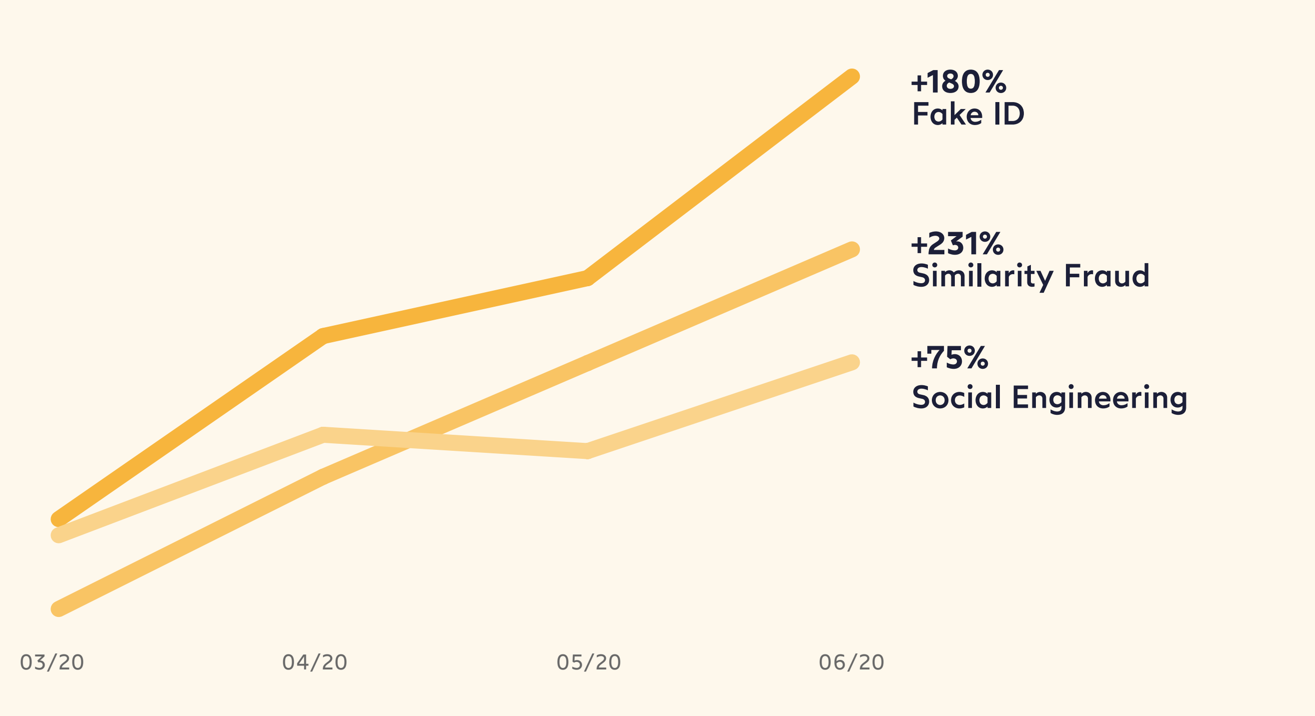
According to a study by the management consultancy Deloitte, 70 percent of decision-makers in German companies see online data fraud as the most significant cyber risk. Not without good reason, because in recent months, there have been a large number of cyber-attacks that took advantage of the global pandemic.

COVID-19 is a significant distraction for management and employees, and large numbers of employees are now working remotely. Criminals use sophisticated analysis to seek out weak spots and to take advantage of flimsy controls and poor IT security. Based on a report by consulting firm PricewaterhouseCoopers (PwC), individual organisations recorded a 40 percent increase in attempted cyberattacks within a week of the first lockdown.

Criminals are trying to exploit the uncertain situation and short-term decisions the government and companies are having to make: there have been numerous fraudulent applications for the state aid programs. The global crisis has fundamentally changed existing trade and payment flows as well. For example, existing business partners must be replaced by alternative providers at short notice. PwC says that criminals will try to use this insight to launder money. For example, in Singapore, where a suspect attempted to launder a million-dollar sum that he had collected through fraudulent trading in medical products.

A massive spike in fraud attempts.

Between March and June last year – when many countries ordered a lockdown to "flatten the curve" of the pandemic – IDnow noticed a significant increase in different types of identity fraud attempts. Similarity Fraud increased by 231 percent, Fake ID Fraud increased by 180 percent, and Social Engineering – already one of the most dangerous fraud methods – increased by 75 percent.



As discussed, criminals are trying to exploit the situation we are currently facing. Many people lost their job due to the crisis, and many Social Engineering attempts have tried to manipulate their potential victims with fake job offers or the promise of a profitable investment with the help of a stockbroker. The victim is asked to open a bank account with the intent to use it for money laundering.

What is Social Engineering?

Fraudsters trick innocent people into registering for a service using their own valid ID. The account they open is then overtaken by the fraudster and used to generate value by withdrawing money or making online transfers.

The innocent parties are contacted by fraudsters directly via Facebook messenger or WhatsApp, for example, or they click on seemingly genuine ads or promotions they find online. They are given a cover story, persuading them to open accounts in return for the promise of payment. The most common cover stories we saw this year were working as 'secret app testers', fake job offers, and bank loans with special conditions.

What is Fake ID Fraud?

Our system has caught and rejected a full range of fake IDs, from low-tech photocopies up to highly realistic, commercially produced fakes. Our research indicates that these are freely available on the dark web for as little as €50, and some of them are so realistic that they can often fool human passport agents. The most commonly faked documents are national ID cards, followed by passports in second place. Other documents, including residence permits and driving licenses, were also detected.

What is Similarity Fraud?

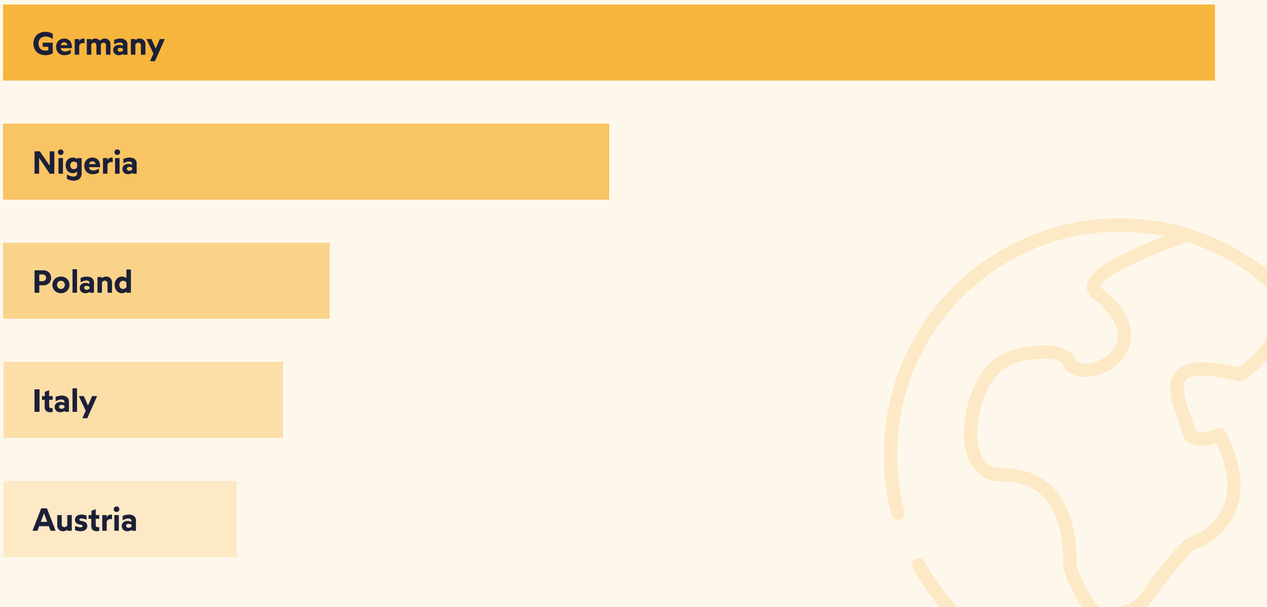
This attempt sees a fraudster using a genuine, stolen, government-issued ID that belongs to a person with similar facial features. It's the modern version of using your big brother's ID to buy beer when you're 15.

IDnow identified a would-be nursing service taking advantage of elderly people in need of assistance to open bank accounts for them. IDnow was able to provide the police with the needed information to stop this organization – of course, in close coordination with the customer providing the banking service.

Working closely with the local authorities is a regular occurrence for IDnow. At the end of last year, IDnow supported the Bavarian police to identify and convict a criminal organisation recruiting bona fide internet users as app testers. These were pretended to be product testers who would check various apps for security and customer friendliness in order to carry out the Video ID process. In fact, however, the testers' personal data and the successfully completed video identifications were used to open online accounts with various credit institutions. The perpetrators have used the generated accounts then for fraudulent online business. In total, more than EUR 560,000 was credited to these accounts.

After extensive investigations, two suspects have been arrested and sentenced to several years of incarceration.

The top 5 countries fraudsters are attacking.



The best of both worlds.

To protect the identity of our customers and users, IDnow utilises the best of both worlds: Modern technology is important, but sometimes human instinct is required. Our qualified identification experts make sure you really are who you claim to be in a simple to follow agent-assisted video call. Constant training guarantees our experts are up to date on the latest fraud methods and tricks.

During the first lockdown, IDnow noticed fraud attempts using fake IDs of unprecedented quality. Our identification experts were able to spot anomalies in the personal security features of these IDs.

To ensure that a customer is not acting under duress, our experts are trained to observe his or her behaviour – has this person got shaky hands, a quavering voice, or are they looking unsettled?

IDnow not only aims to stop fraud attempts, but we also make sure it cannot happen again. Our Quality Management often works closely with the local police to stop criminal organisations and ensures that fake websites are taken off the internet.

IDnow AutoIdent is leveraging modern machine learning technology to enable a highly streamlined user experience. Easy-to-follow on-screen prompts enable very good conversion rates. The verification process is made simple, utilising a familiar selfie-style tool. In case of doubt, our specialists review any unclear cases – combining the best of human instinct and technology.

An essential part of our AI-powered verification process is the so-called "Liveness Detection".

The new IDnow Liveness Detection solution.

The new solution offers an improved False Acceptance Rate. Furthermore, the user experience has been significantly improved based on usage data and user feedback: our previous design required users to rotate their heads, which many found uncomfortable. With the new solution, the user just needs to move his face closer to the camera, and the Liveness Detection will recognise and confirm in less than two seconds that it is indeed a live person's face. This is not only a smooth user experience, but it also provides the highest level of security: even advanced masks, imposters, lookalikes, and doppelgangers can be spotted with a high level of accuracy.

What is "Liveness"?

In biometrics, Liveness Detection is an AI computer system's ability to determine that it is interfacing with a physically present human being and not an inanimate spoof artifact. So, fraudsters using stolen photos, Deep Fake videos, or masks in order to access or create online accounts will be uncovered and stopped.

Trust in AI-powered solutions.

1000%

increased transactions in AutoIdent – from January until June.

IDnow continues to see an increasing trust in AutoIdent – from January until June 2020, transactions have increased over 1000 percent. And based on our expertise, this confidence is justified: with the new Liveness Detection solution, we are able to provide an outstanding user experience while reliably preventing identity fraud.

What is False Acceptance Rate (FAR)?

FAR is a specific key performance indicator that measures false acceptances with a biometric security system. It tracks and evaluates the precision of a biometric system. It therefore determines the rate at which unauthorised users are verified on the system. The lower the FAR is, the more advanced the technology is.

> To stay one step ahead of the latest fraud methods, we need to be faster, better networked and more creative than the fraudsters themselves. To achieve this, we work with a large anti-fraud team that researches in darknet, tests fake ads itself and exchanges information with victims to study the exact methods used by the fraudsters. The team also takes the scammers' websites offline and works together with the police to catch the criminals. On this basis, we continuously adapt our security processes – and rely on a hybrid model that optimally combines AI and human intelligence."

Armin Bauer
Co-Founder and CTO
at IDnow

About IDnow.

IDnow's mission is to leverage its identity verification as a service (IVaaS) platform in order to make the connected world a safer place. The secure ID validation solution from IDnow can be deployed in any industry where companies have online customer interactions that require robust security. IDnow's solutions employ artificial intelligence to validate the presence of security features on an ID document and to detect forgeries. Potentially, the identities of more than 7 billion customers in 195 countries could be verified.

IDnow supports a wide variety of use cases, both in regulated industries in Europe and for entirely new digital business models worldwide. The platform allows the identity verification process to be tailored on a case-by-case basis to specific regional, legal, and business requirements.

Questions?
Let's talk!
+49 (0)89 413 24 600
sales@idnow.de

IDnow.

Potentially verifying over **7 billion people in 195 countries**

Over **280 clients around the globe**

Team of **330**

Founded in **2014**

www.idnow.io

IDnow GmbH | Auenstr. 100, 80469 Munich, Germany | T: +49 (0)89 41324 600 | M: sales@idnow.de