How to Combat Fraud in 3 easy steps

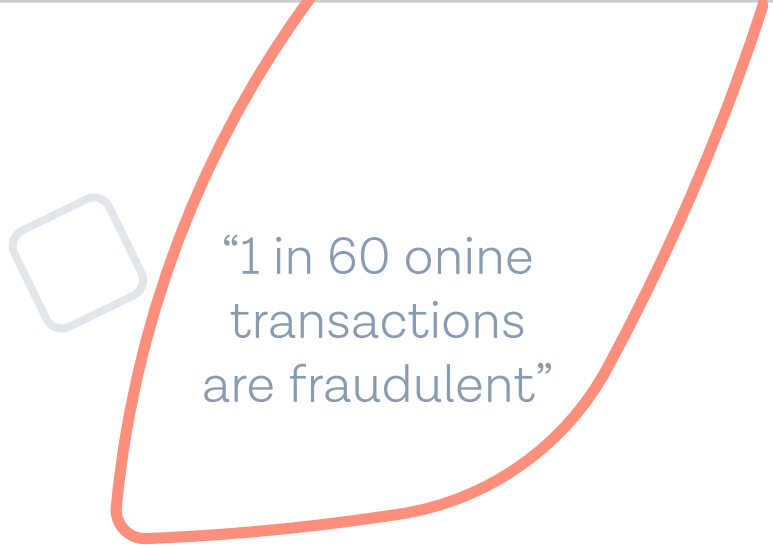
The Compliance Manager's guide to digital KYC

onfido

Contents

onfido

Abstract



Identity fraud is on the rise

Identity theft is the fastest growing crime in the US. Globally, 1 in 60 online transactions are fraudulent. That presents a huge financial and reputational risk for regulated businesses if they get their KYC wrong. As more services move online and fraud techniques mature, document and biometric verification will provide the front line of defense.

Fraud isn’t ‘one size fits all’

With over 4,500 different identity document types in circulation globally, there are countless ways fraudsters can slip through the net. You need to be able to recognize and analyze all of them to keep ahead competitively – and you need to do it quickly, accurately and at scale.

Catching fraud needs human and machine expertise

Identity fraud is a continually evolving game of cat-and-mouse. To keep up, new technologies like biometrics and AI will be key. But just as important is a trained, expert team – especially when it comes to managing 3D documents in a 2D world.

State of play

Identity theft is the fastest growing crime in the US and accounts for half of all reported fraud in the UK, with 1 in 60 online transactions attempted globally being fraudulent.

In the old days, knowing your customer was easy. If people wanted to access your service, they'd do it in person. The risk was low – by meeting them face to face, you could be pretty certain that they were who they claimed to be.
But it is also becoming harder for you to know they are who they claim to be. That's where data comes in. All the information you're able to scoop up about your customers digitally – from their social media profiles, knowledge-based questions or credit bureaus – becomes a proxy for meeting them face to face.

But now that's broken, too. The recent spate of data breaches (there were 1,253 publicly reported in 2017), leaks and attacks shows just how outdated and risky the traditional methods for determining a person's identity really are.
Our personal data – from social security numbers, to bank account information, to passwords – can increasingly be found on the dark web and is available to anyone, at any time. What's more, fraudsters are continually developing more sophisticated techniques. 'Spoofing' attacks – which use a picture of a face from the internet, or even a mask to try and trick facial recognition technology into thinking it's the same person – are common.

That means fighting fraud and truly being confident that your customers are who they claim to be is harder than ever before. More sophisticated, secure and reliable identity verification procedures have never been more crucial. As more services shift from the offline to online, organizations need to master a toolkit that's fit for the new playing field. This includes how they detect and prevent fraud.

While businesses are moving online, the identity verification and KYC processes that they legally require have not been updated to deal with this paradigm shift. Instead, the old processes are being shoehorned into the digital age.

In a space where stakes are high, this is a sure way to lose. Without a system to verify your customers' identities remotely and online, you're at risk of huge fines for non-compliance, reputational damage and competitive disadvantage. So how can you upgrade your KYC and AML for a digital age?

7 ways fraudsters are slipping through the net

In order to comply with KYC and AML procedures it is becoming more common to rely on government-issued identity documents to verify who a person is. But there are a variety of different ways that fraudsters can fake, manipulate or steal them.

There are currently an estimated 4,500 different identity document types in circulation globally. Building a solution that can recognize and analyze all of them effectively is a massive challenge. Add to that the evolving nature of fraud, and that challenge becomes even more complex.

Take this set of six documents. Can you tell which are fraudulent, and why?

Original

Invalid ID Number

Security Feature

Image Editing

Pixel Tampering

Font Verification

onfido

If you're responsible for user onboarding, you need to be aware of all of the ways fraudsters might be slipping through the net – and how you can build a solution to catch them. Here are some of the most common techniques.

1 Forged documents

Fraudsters will illegally change information on the document to enable parts or all of the identity to be modified:

a. Changing the variable information

b. Inserting real pages from another document

c. Removing pages or specific information

d. Applying false stamps or watermarks

e. Digitally altering or adding information on an image of an original document

2 Counterfeit documents

A total reproduction of the original document. Typically a fraudster will obtain a template and insert their own information and photo. These can also be purchased illegally and are a popular option.

3 Stolen bank documents

Unpersonalized original documents are leaked from the manufacturing supply chain and have false information inserted by the fraudsters.

4 Fraudulently obtained documents

Fraudsters lie on their applications (eg use a photo of someone else / apply with a fake document / different personal details). Authorities then issue them original documents containing this false information.

5 Fantasy or camoflage documents

Fraudsters create issuing authorities that do not exist or are not allowed to issue documents. (e.g., Utopia, Rhodesia, British Honduras, World Service Authority, Republic of Texas)

6 Imposter documents

The document itself is original, but is used by someone other than the legal holder of the document.

7 Compromised or sample documents

A government-issued sample or image of documents that are publicly available. (e.g, IDs shared on the web, documents in TV shows or presentations, documents reported as stolen or compromised to the police)

What to watch out for

Within these different types of document fraud, you'll also find different levels of sophistication.

Tier 3

These are poorly manufactured or altered document templates. You can usually detect these cases by looking at data validations, such as document number formats or lack of data consistency within the document.

An estimated 40% of all fraudulent documents are of this variety.

Tier 4

These are unsophisticated amateur attempts at commiting document fraud. These include fantasy or camouflage documents (such as the Global Citizen passport, or British national Identity card) that do not exist.

An estimated 20% of all fraudulent documents are of this variety.

onfido

Tier 2

These are sophisticated document forgeries and counterfeits. All of the data present on the document is correct and makes logical sense, but small variations in fonts, layout and security features are distinguishable to trained experts or a highly optimized technology detection process.

An estimated 35% of all fraudulent documents are of this variety.

Tier 1

These are the most sophisticated attempts at document fraud. These frauds are usually performed by attacking the supply chain of document issuance and manufacture, resulting in stolen blank documents or fraudulently obtained genuines through deceit and social engineering. Also within this tier are the highly sophisticated counterfeits that are available on the black market. These are usually sold for large sums of money and often created by criminal organisations collaborating with governments. These documents can fool even the best-trained document experts, and any machine-based approach. The only way to catch these cases is through extensive analysis of all the documents available to the individual, as well as red flag databases.

An estimated 5% of all fraudulent documents are of this variety. This is increasing as document verification techniques continue to evolve in terms of robustness.

How to combat fraud in 3 easy steps

Knowing what to look for is only one piece of the puzzle. Catching and preventing fraud on your platform is another.

Each fraudulent technique has different fraudulent characteristics, and requires different detection methods. To detect each systematically, you'll need a set of document analytics to inspect each document. These document analytics ensure that the document has not been modified, that it is a legitimate document and that it belongs to the person presenting it.

Evaluating the various aspects of the document image simultaneously requires a wide set of processes. The more sophisticated the fraud technique, the more likely additional techniques will be needed to detect the fake.

onfido

1 Leverage biometrics

Fraudsters want to find a way of committing fraud, and to repeat it again and again. By introducing additional layers of authentication, such as matching the photo in an identity document against a person's biometrics, makes it much harder for the fraudster to be a repeat offender.

But as fraud techniques develop, it's also important to ensure the user is not being impersonated.

Introducing liveness tests into the authentication process can help with this. A liveness test protects against spoofing by checking that the identifying biomerics belong to a real, present person – not just a picture pulled from the internet. Onfido requires a user going through a liveness check to read out three randomly generated numbers and to perform a simple movement, for instance – it confirms that they're alive and presenting the information.

In the future, most transactions that carry a risk will require an identity check involving some form of biometric authentication. Acuity Market Intelligence predicts that by 2022, mobile biometric solutions will authenticate more than 1 trillion transactions annually.

2 Use a hybrid solution

Studies have shown that even highly trained humans aren't very successful at spotting fraud. Human agents have particular trouble matching unfamiliar faces, with recent studies finding about a 17% error. And experience doesn't seem to improve their performance: cashiers average 50% error, police officers 20%, and passport officers 14%.

Clearly, technology is needed to support in fraud prevention – but that's not foolproof, either. While algorithms are better at detecting fraud in still images of faces, humans are superior when it comes to videos and edge cases.

Using a combination of both is best – not just for accuracy, but for speed and completion, too. A fully automated solution might process more documents, more quickly, but it'll reject anything it doesn't recognize. Add in an expert human team to train the technology on new documents and fraud techniques, and you'll see a dramatic uplift in completion rates.

In short, it means more legitimate users can be onboarded, with lower risk of fraud losses down the line. Bitcoin exchange company Coinfloor had a 72% decrease in fraud rate within 6 months of switching to Onfido's hybrid approach combining machine learning and human verification.

3 Know how to handle 3D documents

You need to be sure that the ID presented by users belongs to them. Identity documents designed for verification in a 3D world through touch and light need to be accurately verified through a 2D scan – and that's a challenge. Machine learning models can already detect sophisticated tampering, but the fraudsters are keeping pace. While some solutions are great at analyzing one document type, they've often just hard-coded rules based on common knowledge. It's important to continually develop models so that they can keep track of and keep up with the latest fraud tactics.

While liveness detection has gone a long way to weed out impersonators, sophisticated fakes are the next big challenge. Onfido's defence against such attacks is based on machine learning methods, which detect video attacks based on texture analysis that identifies when a video is displayed on a digital screen.

Onfido Fraud Consultancy

There are over 4,500 different types of identity document in circulation – and fraudsters are always developing more sophisticated fraudulent identity documents to gain access to sensitive data, systems, or even countries. For your business, ensuring that your users' identity documents are not fraudulent is about more than just meeting regulatory requirements and avoiding fines. It's about building trust in your community.

Solution Overview

With over 20 years of combined expertise, Onfido's Fraud Consultancy team is led by Michael Van Gestel, an expert in ID Document security and fraud. Through interactive workshops, our Fraud Consultancy team focuses on highlighting different types of fraud, and training your team on how to analyze identity documents. The comprehensive workshop also lays the foundations for profiling impostors.

onfido

Workshop Overview

Fraud awareness - How prevalent and impactful fraud is

Types of fraud - How do experts classify a fake document and why it matters.

Mechanical printing techniques - Session about the way documents are made

Digital printing techniques - Session about the way documents have PII added

Document investigation - Define your own process for assessing documents

Profiling/Impostors - What is an impostor and how can you identify one?

Revolut

Metrics

81% of agents were more confident in their knowledge of the security features of ID documents

87% of agents are able to more effectively evaluate high risk ID documents

Almost half (47%) of agents were able to lower their average ID processing time

onfido

Michael van Gestel - Global Document and Fraud Strategy - A leading expert in ID Document security and fraud, Michael heads Onfido's Global Document and Fraud Strategy Team. Prior to Onfido, Michael worked as a Document Expert and international trainer at several global document checking and referencing companies. He has also served as a ID Document Authentication Expert/ trainer at the Expertise Centre Identity Fraud and Documents (ECID), sharing his knowledge with embassies, consulates, airlines, security agencies, immigration offices and police departments all over the world.

Dimi Radu - Document Research Specialist - One of the first 10 employees at Onfido, Dimi has a comprehensive understanding of business processes and the wider ID document and Identity industry. Building on his unique technical expertise, Dimi is currently responsible for document fraud research, testing, training, and, implementing product enhancements.

Get in touch:

info@onfido.com
https://onfido.com

onfido

London | **San Francisco** | New York | **Lisbon** | New Delhi | **Singapore**