intellicheck

Running an Effective and Complete Identity Validation Program

WHITE PAPER

Fraud and risk management are big businesses, and the proof is all in the numbers. In 2020 alone, there were over 1.3 million cases of identity fraud, tripling in just two years. In the United States, 33% of adults have experienced fraud in some capacity. That is twice the global average. Of that fraud percentage, 45% can be attributed to new account credit card fraud (Insurance Information Institute).

So, how are fraudsters able to get away with this much criminal activity? It all boils down to a lack of proper validation, verification and on-going authentication processes in place.

A top-notch process needs to be secure, highly accurate, and also must keep the customer experience seamless. With fraudsters continuing to refine their craft, it's even more crucial that organizations don't leave themselves and their customers vulnerable to become victims of fraud.

Types Of Fraud: A Few Examples

Whether it's physical or digital, fraudsters are using fake identification or stealing real identification to get access to services and goods that they should not have access to. Fraudsters use a variety of techniques, including:

Account takeover: This is where a fraudster gets enough information to log into an account. Typically, they will get their information from the account owner via phishing or tricking someone into giving up personal information, or they will simply buy it on the dark web. From there they change the information to make it their own so that they can use it.

Identity Theft/Fraud: When someone/something steals your personal information and uses it without your permission/knowledge

Synthetic identity: This is where a user takes a variety of real information and puts it together to create a fake identity.

Money muling: Fraudsters use this method to target people to coerce/trick them into thinking they're doing a legitimate job. Although the scammers trick individuals into moving money, the "mules" end up being part of a money laundering crime without realizing it.

Friendly Fraud/Chargeback: Occurs when a purchase is made using a credit card and a fraudulent request for a refund or chargeback is made. If the chargeback gets approved, the bank cancels the transaction, and the consumer gets a full refund.

Fraudsters can buy real ID information, harvest and steal a physical ID or have a fake ID created for them. Techniques are easier if faulty validation measures are a factor both in the physical and digital markets.

Depending on the business, there are a lot of ways for a fraudster to get in the front door. For instance:

Buying information off the dark web should be enough for a fraudster to beat a system that only checks static information such as name, address, and social security number.

Buying a highly accurate fake ID is enough to beat a system that relies on the human eye to weed out the fakes.

Businesses, on the other end, face a lot of competition. Not only does competition drive stronger service quality, but it can also drive down service prices. The pressure to improve customer experience to beat the competition and less money to spend on identity validation systems reduce inconvenience at the expense of catching fraud.

Identity Validation & Verification

Identity validation and verification are all about understanding if the individual is who they say they are. Your business might need to identify who you are working with for regulatory compliance reasons or to minimize fraud and risk management. Understanding who you are working with typically involves one or more of the following components:

Document Authentication

Typically a computer-driven optical process to scan documents and match them against a database of valid documents. It can also be used to match a photo in a document to a selfie.

Biometric Authentication

Facial Matching uses technology to match the user with the image on the identity document. Liveness Detection helps ensure that the user is actually present during the transaction and not just presenting a static photograph.

Knowledge-Based (KBA) Authentication

Verifies a person's identity through security questions, that, in theory, only the user knows. This is usually done to match a user to an account, over the phone or online.

Optical Character Recognition (OCR): OCR

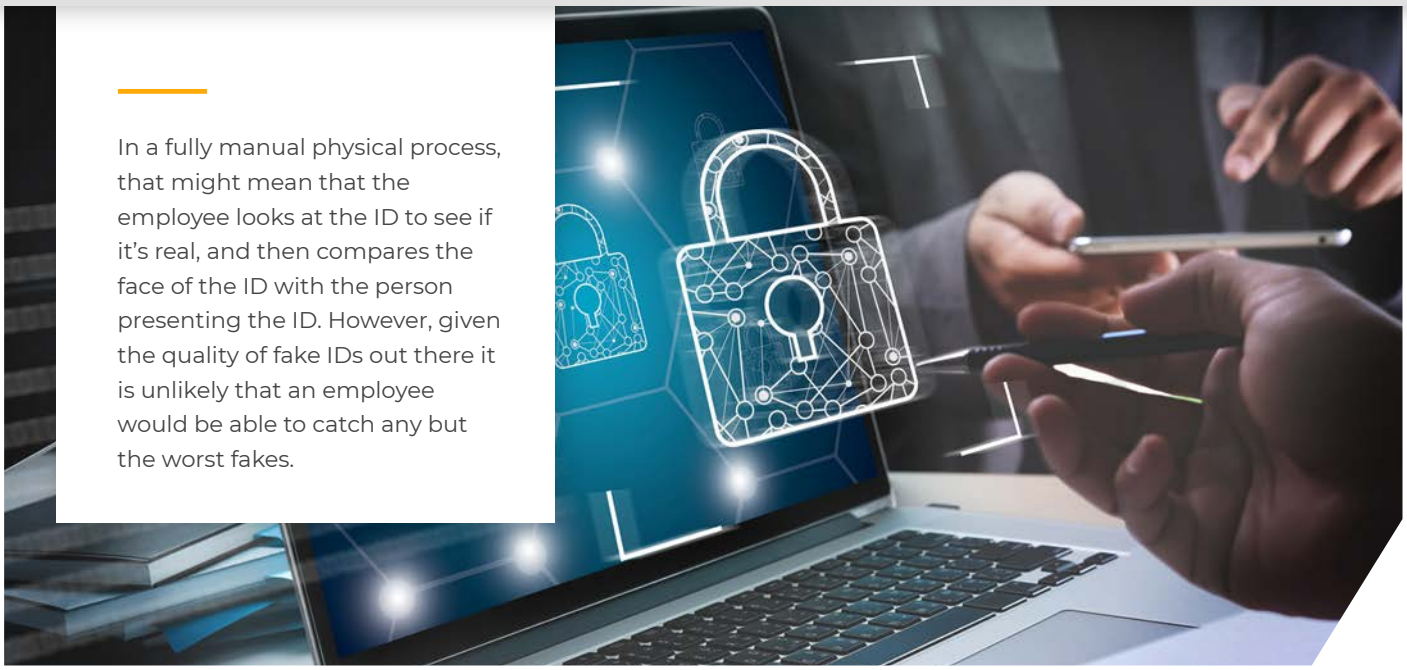
OCR is focused on identifying and extracting the text in a document and using it to fill in a form or for additional security checks. These security checks can include matching it to what is encoded in the document or matching it to third-party databases.

Two/Multifactor Authentication

Requires a consumer's phone or email during the authentication process as a code is sent to them to verify their identity.

Manual Review

This can be done online or in-person, and relies on employees to manually/visually review identity documents.



In a fully manual physical process, that might mean that the employee looks at the ID to see if it's real, and then compares the face of the ID with the person presenting the ID. However, given the quality of fake IDs out there it is unlikely that an employee would be able to catch any but the worst fakes.

Generally, the digital path will involve having the presenter of the ID take a picture of themself. This can be a slower process due to the extra steps including the separate data collection point, and it maxes out at 70% accuracy. This means that one out of 5 times the results are not accurate leading to a good prospect being kept out or a fraudster being let in. The big issue is that the technology applied is only able to determine if the document looks real, not if it actually is real.

Successful Identity Validation & Verification

The goal of any identity validation and continuing verification process is to maintain a trusted space for your best customers to do business. The trick here is to keep the friction at a tolerable level while maintaining security.

Retail

A typical fully manual process for retail identity validation often involves an employee looking at a driver's license and visually matching the image on it to the user.

Online

For online processes, technology has always been the only way to go. This means having the user present information, such as a social security number and/ or an identity document like a driver's license. Technology will verify the document. From there, the user is asked to take a selfie to match the person on the ID with the person presenting the ID.

Call Center

Call center processes typically leverage KBA or knowledge-based authentication principles where the person is asked to answer a security question or verify their address, social security number or a similar piece of information.

The Risks

The wrong information and the wrong process can lead to openings for fraudsters:

- Social security numbers are not effective for verification because they can be purchased for next to nothing on the dark web.
- Not using an ID document means that the presenter can't be matched to the information.
- Security questions to validate the caller does not work on one-off transactions, as it's easily compromised static information.
- With the sophistication of fake IDs, visually assessing a document is not effective.

Technology Benefits

Validating an ID with a technology-based process leads to a dramatic process improvement and effectiveness processes as it:

- Can catch details that the human eye can't.
- Works around the clock at high volumes.
- Consistently stops more fraud.
- Provides the ability to capture information for compliance purposes and can fill in forms for more efficient processes.
- Yields far more accurate results than a social security card number, a driver's license number, or any other combination of static information.

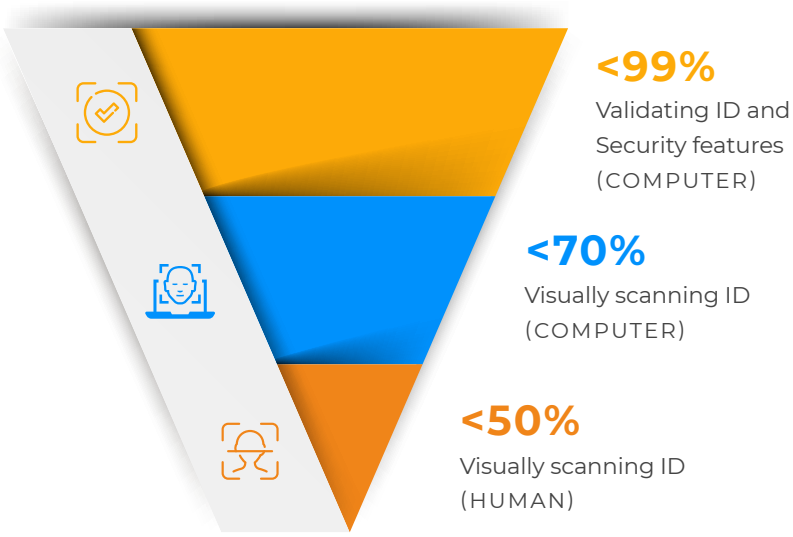
However, not all technology is the same... there is more than just operational efficiency at play.

Friction And Accuracy "The Balancing Act"

Just the right amount of friction is key when addressing identity validation, verification, and authentication.

It represents the extra steps that are involved in the identity vetting process. These steps might be any of the steps noted earlier in this guide. The balance is key and should be constantly revised.

How do you achieve the balance? The balance comes from accuracy.



Each step in the process provides further assurance that the ID has been correctly accessed and to a comfortable level. Fewer steps mean that you have accurately accessed the ID early. However, most businesses stop after a few steps.

For retail businesses using a manual technique it's two steps - look at the ID, look at the person. For digital processes, it is to process the ID and then run additional steps such as a selfie.

If you are lucky it will get you close to **70% accuracy**. In this case, more steps are greater assurance.

Let's look at that 70%

Obviously, an automated solution is far better than an easily beaten manual process, and it is far better to validate the ID than easily stolen and cheaply acquired static information. However, that 70% means that in one in five cases the business has incorrectly identified a good customer and/ or a fraudster leading to more good people turned away and more fraudsters being let in. Any one of those fraudsters can cause tremendous damage in terms of financial losses, stolen identities, and poor business reputation.

Ultimately the best solution is one that does not look at the outside of the document to determine if it looks real. It's the solution that **truly validates and verifies** the document to let you know that it is real and the person is truly who they say they are.

About Intellicheck

Intellicheck is the leader in identity validation and deeply passionate about making sure you can trust that people are who they say they are. We've invested years designing and developing a real-time SaaS platform to tackle this problem. Working, along the way, with ID issuers to ensure that we read the encrypted data within an ID.

Our unique approach to identity validation delivers certainty, detecting fraud and fake IDs most every time. The result is a platform that helps top companies eliminate fraud, fraud losses and retain their brand reputation. Our customers include:

5 of the top 15
banks and card issuers

30,000+
retail locations

Over 60 law
enforcement agencies

Our technology is simple to deploy, easy to use. Making the identity validation and verification process effortless for you and your customers.