Online Face Verification in Insurance:
5 Ways to Enable Digital Transformation

Contents

Overview

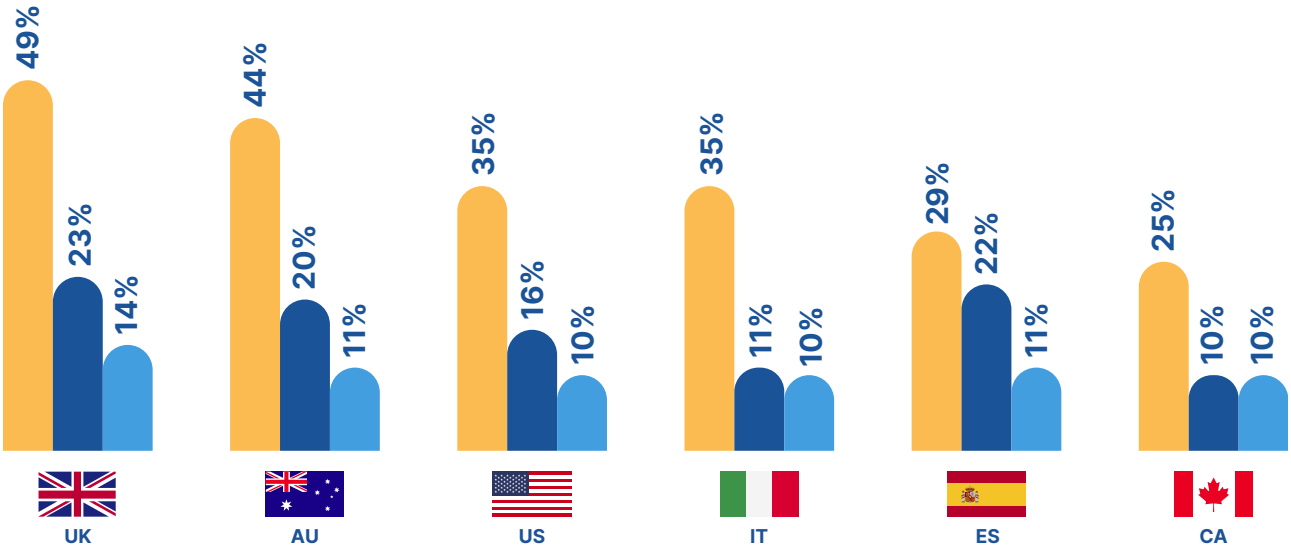
Protect against online fraud. Deliver a secure yet effortless digital customer experience. Comply with regulations. Maximize customer inclusion and accessibility.

These are just a few of the advantages that remote biometric face authentication can deliver to the insurance sector. This report looks at why and how insurers should use biometrics to verify and authenticate customers online, particularly for high-value insurance products such as pensions and annuities.

The need for digital transformation in insurance

The insurance sector has taken longer to embrace digital transformation than many other sectors. This is for a number of reasons, including the preference for personal relationships when dealing with insurance and the complexity of the purchase process, particularly when it comes to pension and annuity products.

However, there is no doubt that consumers are buying insurance online, as recent survey data from iProov shows:



What is driving digital transformation in insurance?

Consumers and insurers stand to benefit from the digital transformation of services:

How can biometric face verification help insurers?

This document looks at five areas where biometrics can help:

1. Confirming proof of life
2. Improving access to online portals
3. Reducing the risk of account takeover
4. Know your customer at onboarding
5. Build trust online

1 | Confirming proof of life

In 2017, French police made a rather grim discovery: in an old freezer at the bottom of a woman's garden they found the body of her 90-year old mother, who had died 10 years earlier.

The daughter had concealed the death and hidden the corpse so she could continue to claim a pension worth around $2400 a month. The daughter had even moved house during those 10 years and taken the freezer and its gruesome contents with her.

This might be an extreme example but all around the world fraudsters are claiming pensions and annuities for deceased relatives, roommates, or people they've been caring for.

The COVID-19 pandemic has exacerbated this issue. Insurers and government officials have been unable to ask individuals to present themselves physically to confirm proof of life, nor has it been possible to ask for a 'life certificate' notarized in person to prove that they are indeed alive.

However, age and infirmity often prevent the claimant from attending in person anyway and those living abroad also present challenges. In a digital world, all customers should be offered the convenience of an online service.

So how can insurers validate proof of life for remote customers? And how can they do that in a way that protects against fraud?

Biometric face verification offers a secure, convenient and inclusive means of confirming proof of life remotely. A simple face scan on a mobile device or computer enables financial services providers to verify the identity and 'liveness' of an online user.

iProov's Genuine Presence Assurance enables insurers to confirm that a user is:

- **The right person** – does the physical face of the person completing the online verification match the face held in a trusted document, such as a driver's license or passport? Are they who they claim to be?
- **A real person** – are they a live human being and not a photo, mask or other attempt to spoof the system?
- **Authenticating right now** – are they completing this process in real-time and not a replay of a previous authentication or a deepfake used in a digitally injected attack?

Deepfakes represent a very real and growing threat to insurers when it comes to proof of life. Instead of keeping corpses in freezers, fraudsters can use deepfake technology that is readily available to create 'deepfakes of the dead'.

A photo of a living or dead person can be animated and made to say or do anything with just a few clicks. This is a global problem and one that is growing.

However, iProov's Genuine Presence Assurance combats deepfakes by discerning between real facial identities and those replicated using deepfake technology. Our proven technology protects against identity fraud while being effortless for the user.

2 | Improving access to online insurance portals

How often do your customers log in to your online portal? Even for home and car insurance products, 30% of customers say they rarely speak to their insurer.

For pensions and annuities, many customers will rarely access their account online. So what happens when they do want access? How do you ensure that the right person is able to access their account without frustration?

The frustration can be caused in many ways. Passwords can be forgotten, email accounts may have been deleted, recovery email addresses or security questions forgotten and phone numbers changed.

Biometric face authentication removes the need for passwords or other online security methods that can be forgotten over time.

Instead, a new customer might verify their face against a trusted document (such as a driver's license) when they open their account. They then use a simple face scan on their mobile device or computer to authenticate themselves whenever they return to the portal.

Alternatively, existing customers can be asked to verify themselves using a trusted document when they next access the portal to complete a sensitive transaction. Future authentication is then completed simply and securely using a face scan lasting a few seconds.

This means that whether your customers visit your online portal once a month, once a year or once every five years, their face will ensure simple, secure access without any fuss or hassle.

This delivers the highest levels of security, protecting both the insurer and their customers from online fraud and identity theft.

A cautionary tale on passwords: a San Francisco man has amassed $240m in Bitcoin but can't remember the password to access it. He was given 7,002 Bitcoin when they were worth a few dollars each and stored them in a digital wallet on a hard drive. He wrote the password on a piece of paper, which he then lost. He has used up eight of his password attempts and only has two more guesses left before the password will encrypt itself, making the wallet impossible to access. Biometric face authentication could have helped him, as he wouldn't have lost his face. It's true that most organizations would be more sympathetic – however, it's a story that demonstrates the limitations of knowledge-based authentication.

3 | Reducing the risk of account takeover

In the previous section, we saw one of the downsides of infrequent interaction between insureds and insurers: the customer forgetting their security credentials to access their account online.

But there's another potential downside to infrequent contact: the customer not noticing when fraud has been committed against their account.

Pension and annuity funds are a target for criminals because of the high value of their contents. By impersonating the policy holder, fraudsters can take over an account and gain access to large amounts of money. Because the true account holder may only check their account once a year or less, account takeover fraud could go undetected and unreported for some time.

It is therefore imperative for insurers to tighten up defenses around pension and annuities.

Biometric face authentication helps to prevent account takeover fraud. A criminal can steal knowledge-based security information, such as passwords and mother's maiden names. They can dupe people into revealing PINs and special words. Once they have that data, they can change phone numbers so that an individual's mobile device can no longer be trusted.

Criminals cannot steal a face, however. They can copy a face, using photographs or videos or masks. But iProov's Genuine Presence Assurance enables insurers to confirm that an online individual completing a biometric face authentication is the right person, a real person and that they are authenticating right now. This ensures that the person logging into their insurance account is indeed the verified policyholder.

Imagine this scenario:

A policyholder has a pension that they pay into regularly through their paychecks. They rarely check or access their pension account.

A fraudster gains access to the account. They could have obtained a password and username from a data breach on an unconnected site. Alternatively, they could have used social engineering to dupe the genuine holder into revealing security data over the phone.

In either case, the criminal then poses as the policyholder and logs onto the online portal, where they can change the holder's address, phone number and email address. After that, any security checks, such as one-time passcodes sent to a mobile device, are compromised as the genuine holder is no longer receiving the alerts.

Years later, when the true policyholder tries to access the account, they find that they have been locked out. When they do get access, the funds are missing.

4 | Avoiding money laundering at onboarding

Insurers have three main priorities when onboarding customers to a new policy online:

1. Provide an intuitive user experience to ensure completion
2. Protect customer privacy and security
3. Comply with regulations

This can be a challenge. Making it simple for customers to purchase an insurance policy has to be balanced with checks to ensure that the policy is not being used for money-laundering.

Criminal networks use insurance policies to 'launder' ill-begotten financial gains by depositing large sums that they then draw down, turning fraudulent money into clean money.

An example of money-laundering in insurance:

A criminal wanting to launder money through the international financial system could buy a life insurance policy using funds from one or more bank accounts. These accounts would likely be based overseas and the amounts would be small enough to avoid attracting the attention of the insurer's fraud teams.

The criminal would then cash in the policy early and request for the funds to be returned to another bank account, often in a different country.

To combat this, regulated insurers and other financial institutions have to comply with anti-money laundering (AML) regulations when they onboard customers.

iProov's biometric authentication technology enables insurers to meet Know Your Customer (KYC) guidelines during online onboarding. A customer verifies their identity by scanning a trusted document (such as a driver's license) using their mobile device or computer. A brief face scan then matches the person's physical face with the image in the document. This ensures that the individual is a real person and that they match the identity contained in the document, without requiring an in-person check.

5 | Enabling insurers to build trust online

Insurers win and retain customers through trust. That trust is fundamental to the long-term success of any insurance brand.

High-value pensions and annuities typically require years of contributions before they are accessed and drawn upon. Customers must feel confident giving their money to an institution that they trust to help them achieve financial security.

If your customers trust your brand, they'll show their loyalty by adding to their portfolio of services and recommending your organization to their friends and family.

It is therefore imperative that insurers demonstrate their commitment to maintaining trust online. It's not easy: the threat landscape changes every day and keeping ahead of the cyber-criminals can be a challenge for any financial institution.

Insurers can build trust with their customers by demonstrating that they take online security seriously by employing best-in-class biometric security authentication and verification technologies.

iProov's Genuine Presence Assurance gives your customers the reassurance that they need. The brief 'ceremony' of the biometric face scan is designed to be completely effortless and passive, yet also provide a reassuring sense of security. Your customers know that secure technology is in place to protect them and their money from account takeover or attack.

About iProov

iProov is the world leader in providing facial biometric authentication technology to financial institutions, governments and other enterprises that need to securely verify customer identity online.

Used for onboarding and authentication, iProov customers include the US Department of Homeland Security, the UK Home Office, the UK National Health Service (NHS), the Australian Government, Singapore GovTech, Rabobank, ING and others.

iProov's unique patented Genuine Presence Assurance technology enables banks, insurers and other financial institutions to ensure that an online customer is the right person (not an imposter), a real person (not a photograph, mask or video presented to a camera), and authenticating right now (not a deepfake or synthetic media attack injected into a sensor or data stream). This provides unique protection against sophisticated digitally injected attacks and the emerging threat of deepfakes. Read more at **iproov.com**.

For more information on how to assure the genuine presence of the **right** person, **real** person, authenticating **right now** contact us at **contact@iproov.com**

contact@iproov.com

iproov.com