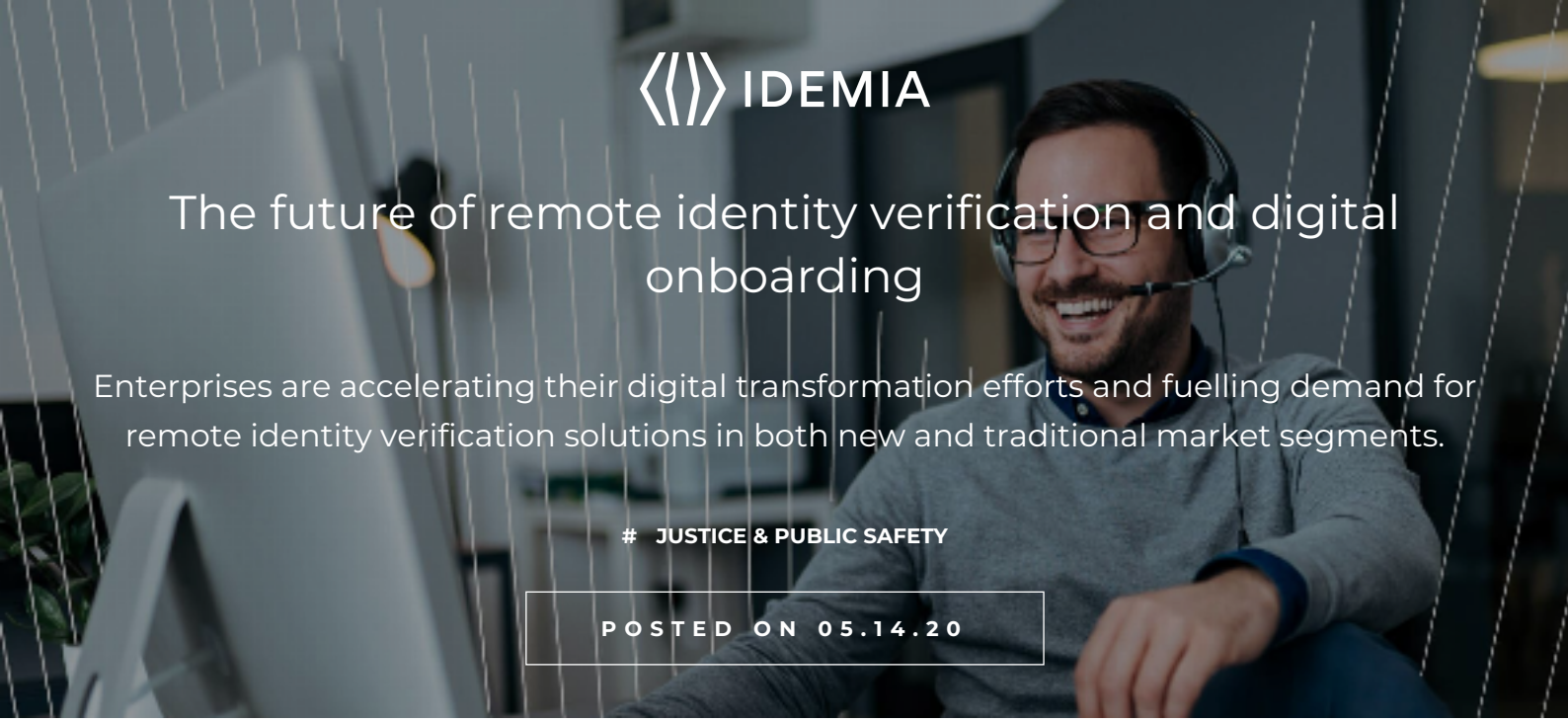

The future of remote identity verification and digital onboarding

Enterprises are accelerating their digital transformation efforts and fuelling demand for remote identity verification solutions in both new and traditional market segments.

JUSTICE & PUBLIC SAFETY

POSTED ON 05.14.20

Identity verification is fundamental to how enterprises interact with their customers. It builds mutual trust between both parties and allows them to perform transactions both online and in-person.

With the global **digital transformation**, many of the interactions that enterprises have with their customers are shifting online, where identity verification must be done remotely. Now banks, mobile operators, and other enterprises must **enroll and authenticate their customers** without ever meeting them face-to-face, and they must do it in a way that is secure, convenient, and complies with regulations.

The benefits of digital onboarding for all enterprises

The need to securely onboard and verify a customer's identity remotely is becoming critical for enterprises. Today, customers expect access to services anytime and anywhere, hence the exponential success of digital and mobile services. In the meantime, identity theft and fraud risks are higher than ever before. The need to securely onboard and verify a customer's identity remotely is therefore becoming critical for enterprises.

Enterprises that have already implemented digital onboarding and remote identity verification solutions have seen the benefits[1]:

- Signing up for an account with insurance companies takes 30 seconds instead of 4 days waiting for a letter with access codes by mail.
- Accessing your credit registration online takes just a few minutes, where previously, customers would wait days for delivery by mail after identification at the post office or bank.
- Healthcare providers can go through an online registration within 10 minutes where previously it could take up to 28 days.
- Taking out a mobile phone subscription now takes a few minutes, where it first took almost half an hour.
- For financial institutions, onboarding new investors takes now just five minutes instead of a few days.

Which sectors benefit from remote identity verification?

Traditional enterprises and service providers can benefit tremendously from remote identity verification. This includes financial institutions, mobile network operators, insurance providers, sharing- and gig economy platforms, eCommerce companies, and online gaming services, just to name a few.

Digital transformation has fueled interest in remote identity verification in some sectors and has sparked the **creation of new use cases** in others.

Telehealth

Telehealth providers enable both patients and doctors to conduct a virtual visit without having to meet face-to-face, reducing the risk of spreading disease to care providers or other patients at a care facility. **Identity verification must be done on both sides to establish trust, verify the patient's identity, and verify their claim for insurance coverage**. Likewise, the health care providers' identities must be verified to ensure that they are licensed and qualified in their field. The global telehealth market was valued at US$31.46 billion in 2018 and is expected to grow at a CAGR of 19.28% by 2025[2] .

Online education

The verification of student identities is an important factor in the successful implementation of a distance learning program. The verification of student identities is an important factor in the successful implementation of an e-learning/distance learning program. The e-learning market will grow by US$90.37 billion during 2019-2023[3]. While a wide array of effective and trusted authentication methods are available, these methods still do not document that the student who is authenticated is actually the one who is taking the exam. **Verifications such as biometric user verification and keystroke recognition (behavioral biometrics) can solve the key challenges in distance/online education**.

Remote hiring

Increasingly, people are looking for remote jobs and prefer working from the comfort of their homes rather than travelling to an office for a desk job. Remote job openings are on a massive growth path — an increase of more than 150% — since 2018[4]. During the hiring process, candidates could present forged documentation depicting fake identities or certifications. **Digital biometric identity verification is essential in curbing these issues, enabling the verification and authentication of a candidate's identity against the provided documentation**.

Remote work

As more and more employees work from home, IT support teams are tasked with password and account recoveries – both of which require a trusted identity. To combat the risk of exposure of sensitive business information or customer personal identifiable information (PII), enterprises must ensure that that all data is secure and protected from data leaks. **Identity verification through biometrics can help to verify the identity of employees accessing this data, regardless of where they are located.**

Government benefits

Unemployment benefits and government programs use digital channels to deliver aid to marginalized citizens or refugees within their borders. To **ensure efficient disbursement and minimize fraud**, the identity of beneficiaries must be established.

A variety of remote identity verification technology solutions

There are different methods of creating a secure, compliant and seamless identity verification solution combining biometrics, document authentication, and other techniques:

- **ID documents**
  Individuals use their smartphone to capture their ID document, passport or driver's license. The data is then verified for authenticity with a trusted third-party or a root of trust.
- **Fingerprints**
  Individuals can use the camera of their own smartphones to capture and verify multiple fingerprints in a contactless and non-intrusive manner.
- **Selfie**
  The individual uses their smartphone to capture a selfie and perform a liveness detection test. **The selfie is compared with the portrait from the ID document** and optionally with a root of trust to provide the highest level of assurance.
- **Video KYC**
  A **live video chat** between individuals and agents can provide a more interactive, guided onboarding way to capture and verify the service user's identity.
- **Behavioral analytics**
  Analyzing the behavioral attributes of individuals including how they interact with their devices, data entry patterns, and more, is a means to detect fraudulent usage of a user's device and account.
- **Voice**
  By analyzing the voice patterns of individuals, it is possible to create a unique voice signature which can be later used to identify and authenticate an individual.

A solution that provides a **secure and seamless user experience** while mitigating fraud and complying with regulations can be the key to an enterprise's success in the market. Combining multiple layers of verification, such as biometric verification and identity document validation can help to combat the risk of identity fraud, **both at the time of account creation and during authentication.**

---

[1] Source: The Paypers, Digital Onboarding and KYC Report 2020
[2] https://www.prnewswire.com/news-releases/global-telemedicine-market-size-was-valued-at-usd-31-46-billion-in-2018-and-is-expected-to-grow-at-a-cagr-of-19-28-by-2025–valuates-reports-300984931.html
[3] https://www.technavio.com/report/distance-learning-market-industry-analysis
[4] https://media.thinknum.com/articles/remote-job-listings-are-growing-faster-than-office-jobs/
