Shufti Pro

Onboarding Remote Employees

How Identity Verification Can Reduce Risks in Hiring Process

White Paper

Table of Contents

Shift From Office-Based Jobs to Remote Working

Before the Covid-19 pandemic, there was already a lot of discussion on the implications of technology for the future of work and the message was clear that the future of work is not pre-determined and it is up to us to shape it. However, the pandemic brought that future much sooner than anticipated as many countries, organizations and workers shifted to remote working to contain the transmission of the virus, dramatically changing the structure of how we work. With this change, remote virtual meetings are now commonplace and economic activity has increased on a range of digital platforms.

According to the International Labour Organization's (ILO) estimate, **before the COVID-19 pandemic, 7.9% of the world's workforce (260 million workers) were working from home permanently [1].** Although some of these workers were 'teleworkers', most were not, including a wide range of occupations, such as industrial workers, artisans, self-employed business owners, and freelancers, in addition to employees. With the spread of the pandemic, the percentage of remote workers has risen tremendously. But the adjustment to remote working is not always so straightforward.

While many companies recognize the benefits of remote work, some have had difficulty making the transition. For instance in Japan, before the 7 April announcement of the state lockdown a survey conducted by the Japan Association with chief financial officers finance directors of various companies found that, **while 96% respondents agreed with**

[1] Voxeu - Work from home

the importance of remote working, 31% of companies were unable to adopt teleworking because the paperwork was not yet digitized and internal rules and procedures necessary for remote working were not ready [1]. Moreover, concerns over the confidentiality of information or possible security breaches or cyber threats can also limit the number of people working remotely.

Amid these concerns of breaches and threats, companies around the globe had to shift to remote working to stop the spread, and more and more companies are now hiring remote employees to keep their operation running smoothly. But bringing new employees on the board remotely is not as easy as it seems. The process involves a lot of challenges for employers, from establishing communication norms for remote employees to making them feel like a part of the team to enhancing security protocols for verifying their identities, there are a lot of challenges an organization or an individual employer has to deal with when onboarding remote staff members.

[1] Voxeu - Work from home

Shift to Remote working

The remote workforce has increased by 140% since 2005. (Global Workplace Analytics)

Remote workers are 35% to 40% more productive (Just remote)

By the year 2028, 73% of all industries will have remote workers (Skillscouter)

32% of people face distraction by social media while working remotely (Vital Smarts)

57% of UK IT experts believe WFH increase data breach risk (Apricorn Survey)

88% of firms encouraged their employees to work remotely during Covid-19 (Gartner HR survey, March 2020)

By 2025, an estimated 70% of people will work remotely at least five days in a month (Vox)

Remote workers save from $4,000 to $7,000 a year in their lifestyle (FlexJobs)

19% of remote employees report loneliness as their biggest challenge. (Buffer)

This whitepaper will discuss in detail the benefits of remote working, risk, and challenges that an organization may face and what part identity verification can play to protect companies from major data breaches and identity theft issues.

Benefits of Hiring Remote Employees

The topic of remote work is producing a lot of attention and many institutions have been conducting their research to find out if work from home is beneficial for organizations or not. According to the latest surveys conducted by the world's leading research institutions including Gallup, Harvard University, Global Workplace Analytics, and Stanford University, remote work can have many positive effects on a company's operations. The common categories where remote working is proving beneficial to includes:

Productivity: Remote workers are an average of 35-40% more productive than their office counterparts, and have measured an output increase of at least 4.4% [1].

Performance: With stronger autonomy through location independence, workers produce results with 40% fewer quality defects [1].

Engagement: Higher productivity and performance combine to create stronger engagement, or in other words, 41% lower absent rate [1].

[1] Forbes - Benefits of remote work

Retention: Around 54% of employees want to change their jobs for one that offers them more flexibility, resulting in an average of 12% turnover reduction after a remote work agreement is offered [1].

Profitability: Companies save an average of $11,000 per year per part-time remote worker or 21% higher profitability [1].

01. Popular tools to ease remote working

Documentation tools

To manage electronic agreements with remote employees and customers online companies can use DocuSign tool, which enables remote recipients to open up contracts on their computers and smartphones and sign them digitally.

Communication tools

The communication tool Slack, lets you interact with your team members effectively and send or receive files no matter how far they are from you. Google Hangouts is another tool that enables you to make video or voice calls with your employees. It can also be used to share important files with remote employees and conduct a virtual meeting with them.

Project management tools

For handling your team's work and projects online, you can use a software as a service (SaaS) tool, called Asana and Google Docs, which is a browser-based word processor that lets you create, edit, and share documents online.

[1] Forbes - Benefits of remote work

Document and identity verification tools

The most important factor of onboarding remote employees is to verify the identity of the candidate applying for a job. Shufti pro helps companies verify their candidates using a hybrid approach of AI and HI technology.

Shufti Pro can also help Human Resources managers to conduct interviews and hire remote employees through its Video interview KYC feature.

Employee monitoring tools

Companies can use remote employee monitoring tools to assign and track tasks, monitor attendance and among other things effectively.

Risks And Challenges Associated With Remote Hiring

Companies that hire remote employees have to face certain risks and challenges that are not associated with office-based workers, which can vary from company to company. But there are a few common risks and challenges every organization has to face who has hired or plans on onboarding remote workers. Let's discuss a few of them in detail.

01. Challenges

Establishing communication standards

While employees do enjoy the flexibility of remote work, it doesn't mean they don't want to be a part of office culture. Remote workers have fewer opportunities to develop that sense of camaraderie or friendship with their colleagues, and they have less visibility into overall company missions and values. As a result, some remote workers experience isolation, loneliness, and dissatisfaction with their roles in a company. So, organizations need to adopt a work-from-home culture that helps remote employees feel that they are a part of the larger company culture as much as possible.

In a research study by Zogby Analytics [1], employees working remotely reported a lack of information from management and timeliness of the information as the biggest obstacle of working from home. It can be a challenging task to coordinate teams made up of employees that are located across different time zones, not to mention the added difficulty of communicating without the tone and body language so crucial for understanding. Such communication issues can negatively affect not only the work productivity but also employee morale. So creative effective communication standards should be a priority when managing a remote workforce of any size.

[1] Zolby Analytics study

Focusing on security protocols

The shift to remote work is often followed by a transition to the cloud, opening organizations up to new security risks, including cyber threats, breaches, hacks, and identity theft. **According to Security Boulevard, nearly 16 billion records have been exposed in companies around the globe till August 2020, with 8.4 billion records exposed in the Q1 of 2020 alone [1].** This number is a 273% increase in comparison with the first half of 2019 during which 4.1 billion records were exposed **[1]**.

Additional challenges related to employee hardware arise when IT managers face the challenge of managing and supporting mismatched devices running on different operating systems. A few remote workers often mix work and personal data on the same device and apps, leading to unintentional exposure to friends and family and online attacks. Moreover, remote data access by employees can cause serious damages, where a hacker can gain deeper access to your organization, exposing you to a host of IT security threats. Once cyber criminals gain privileged access to your system, it becomes difficult to prevent data loss, phishing attacks, and protect against ransomware, etc.

Employee monitoring

Monitoring and tracking of remote employee performance is another challenge that companies have to face, where they have to ensure that all remote workers are managing their work effectively and efficiently. Also, they have to keep a check on people who are performing tasks on time and in-line with company standards.

[1] Security Boulevard

Job performance tracking for remote workers consists of two categories, those who have to complete their work on time and those who have to work and manage their tasks based on the number of hours set for them by their managers. In either situation, monitoring remote employees can be a difficult and frustrating undertaking if you are not prepared.

Identity verification

Identity theft is on the rise and you must make identity verification an important part of your onboarding process, but verifying the identity of remote employees is a big challenge for companies. The candidates applying for remote jobs can present fake documents during the hiring process which can expose an organization to security risks.

According to the HR Research Institute 2019 survey, 40% of respondents reported experiencing at least one instance of identity fraud and 35% of respondents believed employment-related identity theft will continue to climb over the next several years [1]

02. Risks of hiring remote employees

Fake identity and job credentials

During the onboarding process of remote candidates, they are required to submit their official documents to the company so their academic and professional qualifications and achievements may be evaluated against the skills required for a particular job. However, to get hired, those candidates may present forged documents, depicting fake certifications, when in reality, they may not even be half as qualified.

[1] HR Research Institute 2019 survey

Financial security risks

Remote jobs come with a high risk of fraud for the hiring companies. Recruiters may never be sure that a remote candidate will not cause any financial losses to them, by taking their money and not delivering the completed or high-quality work in the promised time. Worse, remote employees may ask for an advance payout and not deliver any work at all. They may remove their work profiles and cease to exist as that entity. In cases like these, a single person has multiple profiles used to scam people at large.

Cybersecurity risks

Home wi-fi security

Contrary to the office environment, where IT managers can control the security of all Wi-Fi networks, home networks from where your employees' are working probably have weaker security protocols (such as WEP instead of WPA-2). This gives hackers a chance to easily hack and gain access to the network's traffic.

Phishing attacks

Phishing attacks are considered as the top cause of data breaches where hackers can easily send seemingly legitimate, deceptive emails with malicious links and attachments. Once an employee clicks on these malicious links, a hacker can gain access to the employer's device.

Insecure passwords

Simple or easy passwords are incredibly easy for hackers to crack, and if that insecure password is used across several accounts, hackers can easily gain unauthorized access to multiple accounts in a very short period.

Data theft

With unsupervised and enhanced access to systems and files, remote employees could steal company data more easily. Breaches of your customer data or proprietary secrets could lead to loss of funds, legal issues, damage to reputation, and lost customers. Employers who work with especially sensitive data, such as healthcare and financial services, should be especially careful when allowing employees to work from home. But employees aren't the only ones who could steal your company's data.

Partners, roommates, family members, or visitors pose a risk to your company's secret or sensitive information. Even if devices and files are password-protected, fraudsters might hack into them, sneak a peek when the employee is typing or gain access when the employee leaves their computer unlocked for a moment.

How Identity Verification Helps in Dealing With Remote Onboarding Risks

01. Remote candidate hiring

It is highly risky to hire a remote employee online and trust him with all the business matters. For remote working opportunities, companies have to hire individuals without directly meeting them beforehand. Candidates are being interviewed online and hired based on what they present. So during onboarding, digital identity verification is very important to secure your company from cyber risks. By using face verification and 3D liveness detection, companies can perform biometric authentication on remote employees before hiring them.

DO YOU KNOW?

Shufti Pro's video interview KYC solution is an all-in-one solution for remote onboarding, companies can interview candidates and perform facial recognition and document verification at a single place.

02. To verify the identity of remote employees

Considering the growing rate of identity fraud in employment-related activities, digital identity verification is essential, to check the identity and the authenticity of the documents presented by the candidates during the hiring process. This can be done by using document

verification solutions. If the potential employee is a scammer, their identity documents like government-issued ID card, passport, driving license or payment cards, may be counterfeit or stolen. They would never present any true information that can be traced back to them in case of an investigation. For combatting these types of frauds, it is essential to catch the suspects before they can assert any harm to the hiring company or individual.

03. Remote access management

Due to the sudden shift towards work from home due to the Covid-19 pandemic, most companies nowadays are opting for cloud storage services to store their data online. But giving access to these cloud storages to remote employees creates a huge risk of data theft or unauthorized access to these storage. To combat these risks companies are integrating biometric authentication and ID card screening processes for remote workers to gain access to these data storage. This can help companies to prevent unauthorized entries and theft of sensitive information.

Shufti Pro's biometric authentication empowered with liveness detection captures a video selfie of the user's face during sign-in and verifies existing presence within the system.

How Shufti Pro Can Help In Verifying Remote Employees

Shufti Pro's easy to use identity verification platform can help companies in various countries to verify their candidates for smooth and secure remote onboarding. Shufti Pro can help organizations deter digital scams, and protect themselves from revenue losses. While performing verifications of your remote candidates, Shufti Pro performs thorough background checks during the onboarding process to screen out individuals that pose a threat to your organization. Shufti Pro utilizes various verification methods to make sure that you only onboard legitimate employees in your company.

01. Identity verification

Shufti Pro's identity verification service helps organizations to tackle the continuous threats of the data breach, identity theft by verifying the legitimacy of employees. It combines Artificial Intelligence (AI) and Human Intelligence (HI) to deliver real-time verification results.

Document verification

Shufti Pro's document verification solution helps companies to enable quick and secure onboarding of remote employees with a 98.67% accuracy rate. It supports 3000+ types of ID documents in 150+ languages and can verify government ID cards, passports, licenses, and credit/debit cards.

Shufti Pro verifies your candidates' documents in 4 simple steps:

- Candidate takes a photo of his identity document in real-time or uploads a photo from mobile/desktop.
- Shufti Pro's solution extracts required information using precise OCR technology.
- AI-powered solution performs authenticity analysis of the ID document and information on it using AI and HI
- Shufti Pro sends verification details to the client via API or back-office.

Document Checks that Shufti Pro performs include:

- Checking authenticity of document format
- Detection of forged/photoshopped document images
- Extraction and verification of information (such as name, DOB, country, etc.)
- Document issue and expiry date verification

AI-powered facial recognition

Shufti Pro's facial recognition technology utilizes AI and HI to perform biometric verification within seconds. The software captures the picture of the customer in real-time and matches the facial checks with the ones stored in the database.

Shufti's facial recognition technology help companies to identify various frauds with the following checks:

Liveness Detection

Microexpressions analysis

3D Depth Detection

Anti spoofing checks

Fake image detection

Human face attributes analysis

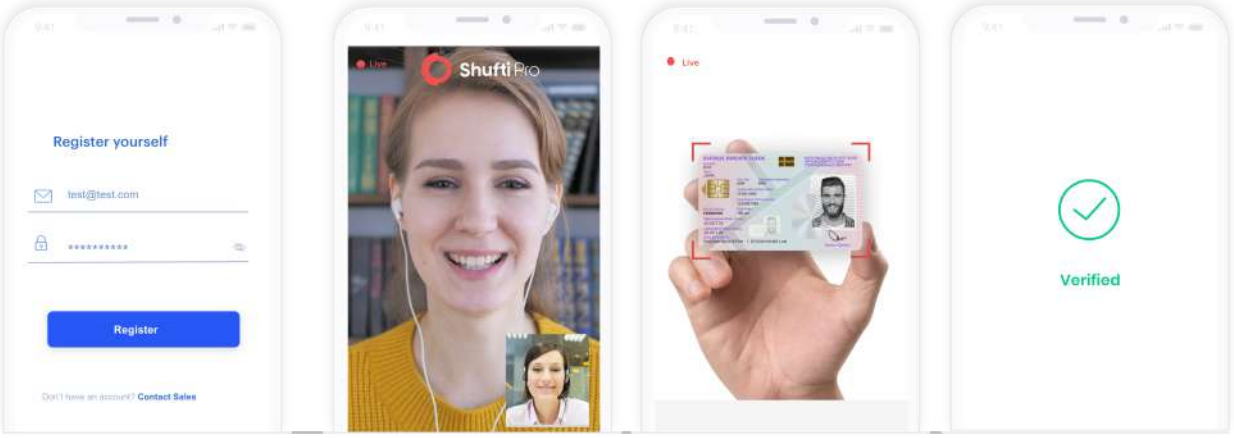
AI mapping techniques

02. Video interview KYC

Shufti Pro's video interview KYC enables swift and secure onboarding by helping companies to perform live interviews of their candidates and live identification process that is faster and guarantees high security. The video KYC feature of Shufti Pro offers:

- KYC expert's live assistance for your remote employees
- Eliminate identity fraud with online verification
- Fast onboarding with human verification specialist
- Fully customizable features based on your industry

Through Shufti Pro's video KYC feature companies can verify their remote candidates in four easy steps:



End-user registers on your platform

Live video call with KYC expert

End-user shows the identity document

Verification results are delivered

Conclusion

While working from home is an important measure for mitigating the COVID-19 pandemic, this norm may continue long after the crisis ends. In any case, one thing that must be kept in mind is that to contain cyber threats or breaches and to fight back fraudsters while working remotely, it is needed more than ever to have a sound identity verification solution. By knowing who you are onboarding as an employee in your company it becomes a lot easier to curb frauds. The only way to be sure about who you're interacting online with is to have stringent measures to authenticate that individual's identity.

Want to verify remote employees before hiring them in your company?

Discuss it with our experts

Apply for a no-commitment **free trial**
Get non-discriminatory access to all features of the selective service of **Shufti Pro for 15 days.**

Get a Free Trial

www.shuftipro.com

sales@shuftipro.com

Shufti Pro True Identity Builds Trust

Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from 3000+ ID templates and business entities from 200 million companies data.