Q5id
You. Proven.

KYE

Who did I hire?

How to Know Your Employee (KYE)
in a world of identity fraud.

q5id.com


Q5id

Know Your Employee (KYE)

During this identity fraud epidemic, it's more important than ever to prove your new hires' identities.

Contents

Click section title to go to that page.

KYE by Q5id goes beyond traditional ID verification by proving the identity of the person, not just verifying the provided ID. A primary goal of KYE is protection. By knowing your employee before they are hired, you can help protect your organization, employees, customers, and reputation.

Executive Summary

Within 15 months, the Federal Bureau of Investigation (FBI) released three warnings about people using deepfakes and synthetic identities to obtain work positions. The warnings highlighted potential consequences resulting from the hiring of fraudulent workers. New hires gain access to corporate and proprietary information, and misuse of this information can expose an organization to multiple risks that can result in financial and reputational harm.

Through the continued advancements of artificial intelligence (AI) and digital technologies, hiring fraud has been elevated beyond only the use of a stolen social security card or a stolen identity. Deepfakes, synthetic identities, shallowfakes, and identity obfuscating are being used to obtain more advanced employment positions not just for their greater levels of increased wages but for potential access to proprietary information that can lead to various forms of fraud. These are also difficult to identify and often need specialized software to detect them.

With the advancements in the techniques used to obtain work positions fraudulently, there has also been a corresponding advancement in mitigation measures. The U.S. Government has been proactive in advising on the strategies and tactics that can be used and they include additional measures for hiring of freelance programmers and developers. Employment fraud is still costly to organizations and occurs even within companies that have conducted background checks.

Know Your Employee (KYE) improves the hiring process by going beyond standard verifications of name, address, and date of birth using an ID. The most significant factor for KYE is the incorporation of identity proofing to prove the person being hired is who they say they are. Identity proofing goes beyond traditional ID verification and background checks by reversing the assumption that when a person provides an ID, that ID is for that person. Through the National Institute of Standards and Technology (NIST), part of the U.S. Chamber of Commerce, an adherence framework for identity proofing was developed for organizations. Within this framework, three levels of identity assurance are used with graduating identity proofing requirements.

KYE by Q5id meets or exceeds NIST SP 800-63A IAL2 standards with their patented identity proofing process. This includes verifying a person's identification and specific attributes of that person and then associating multiple biometrics to those proven attributes. This cloud-based identity proofing process takes just seconds for the client to submit a request to the job candidate and less than three minutes for the candidate to complete. The result is a false acceptance rate of 1 in 933 billion. This can also be stated a different way: the chance of another person having the same biometrics is less than 100 times the population of Earth.

Key Takeaways

The goal of Know Your Employee (KYE) is to protect businesses from hiring fraud.

Hiring fraud has consequences beyond the cost of a new hire, which can include:

- Providing new hire access to customers' personally identifiable information (PII), financial data, corporate IT databases, and/or proprietary information that can expose an organization to financial and reputational risks.
- Lost time and productivity from not hiring the correct person in a position.
- Downtime for customers and employees.
- Damage to an organization's brand and reputation.

Current background check processes involve verifying the identification document (ID) provided by the job candidate, with the assumption that the candidate is the person on the ID.

The FBI has released three warnings on hiring fraud since 2021, related to remote workers.

Types of hiring fraud include:

- Stolen identities
- Skill misrepresentation
- Identity obfuscating
- Deepfakes
- Synthetic identities
- Shallowfakes

Introduction to KYE

Here is a hiring scenario: A recruiter you have not previously worked with before contacts you and offers ten programmers who work remotely and are ready to start. You have been looking to fill multiple positions, so you interview all the candidates. Each programmer can state their relevant employment history, the programs they are proficient in, and their education. Some even have a digital portfolio of their work. You offer each person a position, run a basic background check, and then begin to onboard the new employees into your company. As the weeks pass, your department heads report that the programmers' work is consistently late and subpar or incomplete. After a month, you let them all go. What happened?

The above example demonstrates a recent hiring con to train a group of people on how to respond to basic questions related to a position, set up false identities, and then place them in remote positions with the goal of collecting one or two paychecks before being discovered. Here we see how the remote programmers bluffed their experience enough to get hired and collect their paycheck, while the recruiter also earned payment for the temporary placement.

In a recent study on occupational fraud conducted by the Association of Certified Fraud Examiners (ACFE), employers reported an average loss of $8,300 per month. The types of fraud included financial statement fraud, payment tampering, skimming, payroll, and outright theft of cash.[1]

It may not be just about the wages.

While there was a cost in the example to the employer, it was not just the raw salary. According to Glassdoor, the average US employer spends about $4,000 and 24 days to hire a new worker.[2] But there are additional costs and potential damages beyond the salary and recruiting costs. Fraudulent hires may gain access to customers' personally identifiable information (PII), financial data, corporate IT databases, and/or proprietary information which exposes an organization to financial and reputational risks. Proving job candidates before they are hired will help protect one's organization, employees, customers, and reputation.[3]

Risks an organization can experience include:

- Lost time spent in the hiring process of a false candidate
- Lost productivity by not having the correct person in a position
- Intellectual property (IP) theft and loss of trade secrets
- Downtime for customers and employees resulting from assigned work not completed
- Irreparable damage to the organization's brand and reputation
- Loss of customer loyalty, attrition, and negative customer experience
- Company closure at the most extreme

The risk of data breaches is also a concern for all organizations but it's even greater for those with a remote workforce. A 2022 study conducted by International Business Machines (IBM) noted 28 key factors affecting the cost of a data breach.[4] A remote workforce was ranked 8th for its impact. The study also noted that data breach costs were greatest for organizations with the largest remote workforce.

Today's Hiring Verification Practices and Their Limitations

Currently, any new hire is required to provide the following information about themselves:

- Name
- Address
- Date of birth
- Social security number or other taxpayer identification number

These requirements are part of the U.S. Government's Form I-9, which is used to verify the identity and employment authorization of individuals hired for employment in the United States. Per the Internal Revenue Service (IRS), "All U.S. employers must properly complete Form I-9 for each individual they hire for employment in the United States. This includes citizens and noncitizens."

Within Form I-9, the employee must present to the employer "acceptable documents evidencing identity and employment authorization. The employer must examine the employment eligibility and identity document(s) an employee presents to determine whether the document(s) reasonably appear to be genuine and to relate to the employee and record the document information on the Form I-9."[5]

The extent an employer must go in verifying an employee is in the examination of the provided verification documents that show the required information and then determining if the documents reasonably appear to be genuine. Companies have the option within legal parameters to go further and request additional methods of verification based on the position requirements and security access level to limit the cost and harm associated with a wrongful hire. These methods may include:

- Background checks
- Employment history checks
- Education verification
- Credit checks

Even with the above checks and verifications, a deeper type of employee verification may be needed. In Occupational Fraud 2022: A Report to the Nations, it was found that 57% of organizations conducted a background check on the perpetrator prior to hiring them. Additionally, 21% of background checks on the perpetrators revealed existing red flags.[6] One approach to reducing potential employee fraud is implementing KYE into the hiring process.

The Definition and Genesis of KYE

KYE stands for Know Your Employee and is a recent attempt to improve on the hiring verification process. The concept of KYE is derived from Know Your Customer (KYC), a requirement the financial services industry uses to obtain basic information about their clients. This information includes:

- Name
- Date of birth
- Address
- Age
- Taxpayer ID such as a social security number

The Goal of KYE

The primary goal of KYE is protection. New hires, both valid and fraudulent, gain access to some level of proprietary and confidential information. By knowing your employees before they are hired, an organization can better protect itself, its employees, customers, and reputation.

Globally, cybersecurity spending has been forecasted to reach $174.7 billion by 2024.[7] In this age of remote and work-from-home positions, companies are committing more resources to fraud prevention and improved employee background checks is one part of this process.

In June 2022, the Federal Bureau of Investigation (FBI) published a Public Service Announcement warning that deepfakes and stolen personally identifiable information (PII) are being used to apply for remote and work-at-home positions.[8] The previous year, the FBI also published a Private Industry Notification warning of malicious actors using synthetic content as part of foreign influence campaigns. The same notification also warns of "the use of content generation and manipulation tools to develop synthetic corporate personas or to create a sophisticated emulation of an existing employee." [9]

The two published notifications warned that "the emerging attack vector will likely have very significant financial and reputational impacts to victim businesses and organizations." The FBI releases these alerts and statements to help stakeholders guard against the ever-evolving ransomware threat environment. These advisories, FBI Flashes, FBI Private Industry Notifications (PINs), and joint statements are designed to help cybersecurity professionals and system administrators guard against the persistent malicious actions of cyber threat actors.

In 2022, Meta, previously known as Facebook, released in their Quarterly Adversarial Threat Report #1, that the company "took action against multiple countries in the Middle East that used well-resourced and persistent operation while obfuscating who's behind it. This cyber espionage campaign's goal was to steal credentials by creating fake accounts and fictitious personas. Some of the personas posed as human rights activists and academics." [10] Meta also reported on a network of fictitious corporate recruiting sites that were engineered to produce malware downloads "likely in an attempt to gain information and access to corporate systems."

The FBI also called out synthetics in their 2021 Notification stating, "Synthetic content may also be used in a newly defined cyberattack vector referred to as Business Identity Compromise (BIC). BIC will represent an evolution in Business Email Compromise (BEC) tradecraft by leveraging advanced techniques and new tools. Whereas BEC primarily includes the compromise of corporate email accounts to conduct fraudulent financial activities, BIC will involve the use of content generation and manipulation tools to develop synthetic corporate personas or to create a sophisticated emulation of an existing employee. This emerging attack vector will likely have very significant financial and reputational impacts to victim businesses and organizations."[11]

Types of Hiring Fraud

In 2007, AMC premiered the television show "Mad Men", a fictional series about the world of advertising on Madison Avenue in New York City. The show was set in the early 1960s and its key protagonist, Don Draper, was an advertising protégé that started at the bottom of the industry writing copy for a fashion company. The character proceeded to dominate the advertising industry over the next decade and Don Draper becomes a successful businessman. However, Don Draper was not who he claimed to be. The real Don Draper was killed in a Korean War bomb attack and fellow serviceman, Richard Whitman, who was injured in the same attack, saw this as an opportunity to trade places by exchanging dog tags. His identity was replaced.[12]

A stolen identity in 1952 would have been relatively unsophisticated but possible with that time period's limited technology. Today, stolen identities are still used to fraudulently obtain jobs. But hiring fraud has drastically advanced and now mimics the imaginations of the best science fiction writers. Artificial intelligence (AI) is now being harnessed to replicate and even create alternative identities.

Stolen identities are so common that in the most recent review of employment-related identity fraud published by the United States Government Accountability Office (GAO), they identified 818,000 cases in 2018 where there was a mismatch between Form W-2 (Wage and Tax Statement) and the identity on the tax return.[13]

Let's examine the growing sophistication of the methods used to conduct hiring fraud.

Stolen Identities

This is the most common identity theft where someone steals your personal information to present themselves as you. The person can apply for credit, file taxes, receive medical services, and in the case of employment, obtain a job.

Skill Misrepresentation

The purposeful misrepresentation of the skills of one or a group of workers with the goal of being hired to obtain access to an organization's proprietary information in addition to salary. (There is an example of this in the introduction to this white paper.)

Identity Obfuscating

Involves workers deliberately obscuring their online identities, locations, and nationality, often using other names as aliases. To further conceal their identity, these same workers may additionally sub-contract work to others. One of the main goals of identity obfuscating is to evade detection by fraud prevention, sanctions compliance, and anti-money laundering measures. [14]

Deepfakes

A deepfake uses AI and machine learning to manipulate visual or audio content for the purpose of deception. Most commonly, this is a video of a person in which their face or body has been digitally altered so that they appear to be someone else. There have been FBI warnings on the increased practice of using deepfakes in obtaining work positions.[15]

Synthetic Identities

As with deepfakes, synthetic identities also use AI content generation and manipulation tools. This is then combined with various Personally Identifiable Information (PII) from one or more real people that are combined to create a new, synthetic persona instead of mimicking an existing person.[16]

Shallowfakes

Also known as cheap fakes, shallowfakes are defined by Europol as "videos or audio recordings that are either presented out of context or are doctored with simple editing tools."[17]. Within the hiring context, shallowfakes can be used to misrepresent an employee's skills through manipulated work samples.

> ***A stolen identity in 1952 would have been relatively unsophisticated but possible with that time period's limited technology. Today, stolen identities are still used to fraudulently obtain jobs.***


FACIAL RECOGNITION

Deeper Discussion on Stolen Identities

In the most recent review of employment-related identity fraud published in 2018 by the United States Government Accountability Office (GAO), 818,000 cases were identified where there was a mismatch between Form W-2 (Wage and Tax Statement) and the identity on the tax return.[18] While a portion of this mismatch may be a clerical error, the high number highlights the many potential cases of someone using another's social security number to work and generate a W-2.

What is a Stolen Identity?

Stolen identities are the most common form of identity theft. They usually involve the theft of one's personal information such as their name, social security number, or date of birth. This information is then used to present themselves as that person. The fraudster can then apply for credit, file taxes, receive medical services, and in the case of employment, obtain a work position.[19]

How stolen identities are used in hiring.

Stolen identities are common in low wage positions such as farming and restaurant work. The applicant may not have legal work documentation and therefore uses someone else's identity to apply for a position. More serious uses of stolen identities occur when used to obtain employment positions that gain access to an organization's proprietary information including financial data, IP, trade secrets, and even customers' Personally Identifiable Information (PII).

The above identity mismatch example generated a strong response from GAO, producing a recommendation to both the IRS and the Social Security Administration (SSA) to consider new ways to check for identity fraud and to expand on enforcement. They also recommended that the SSA and IRS improve their communication on the sharing of wage data.

Despite the recommendations by GAO with no hard deadlines for implementation, organizations will have to continue to manage how they protect themselves from hiring fraud and any negative consequences as a result.

Deeper Discussion on Identity Obfuscation

In 2022, the U.S. Department of State, the U.S. Department of the Treasury, and the FBI issued a joint advisory for the international community, the private sector, and the public. This advisory discussed attempts by the Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) to obtain employment of their information technology (IT) workers while posing as non-North Korean nationals including South Korean, Chinese, Japanese, Eastern European, and U.S.-based teleworkers. These DPRK IT workers deliberately blurred (obfuscated) their identities, locations, and nationality online, often using non-Korean names as aliases.[20]

What is Identity Obfuscation?

Obfuscation can be defined as obscuring the true meaning of something.[21] We define identity obfuscation, in identity management terms, as masking the identity of someone using computer code.[22]

How they are used in hiring

In the above advisory, DPRK IT workers routinely use counterfeit, altered, or falsified documents, including identification documents, and forged signatures—either ones they created themselves using software such as Photoshop, or by hiring a document forgery company to alter, combining the IT worker's own or a provided photo with the identifying information of a real person. DPRK IT workers commonly procure forged documents such as:

- Driver's licenses
- Social security cards
- Passports
- National identification cards
- Resident foreigner cards
- High school and university diplomas
- Work visas
- Credit card, bank, and utility statements

Through the production of forged documents, DPRK IT workers can create, steal, or mask an identity to apply for and obtain remote positions.

In some instances, these identities are stolen, while in others, the DPRK IT workers have solicited non-North Korean nationals to set up accounts using their own personal information

or information that they can access. Control of the accounts is transferred to the DPRK IT workers for a fee. This allows the DPRK IT worker to conceal their identity when bidding on and completing freelance projects for clients online, using the infrastructure of the real account holder via remote desktop access. Each IT worker often uses multiple identities and accounts, which can also be shared between IT workers on the same team. These accounts and identities purport to be from countries from every part of the world.[23]

Risks beyond access

While there is general risk when hiring any new employee due to access that is granted to new employees, the risk is magnified when the hiring involves IT-related employees. These new hires may also gain some amount of access to an organization's proprietary information and backend computer systems. Using the above case about companies unknowingly hiring DPRK citizens, we also see potential risks going beyond access. Companies also face reputational risks and the potential for legal consequences, including sanctions designated under U.S. and United Nations (UN) authorities, for individuals and entities engaged in or supporting DPRK IT worker-related activity and processing related financial transactions.[24]

Deeper Discussion on Deepfakes

In the summer of 2022, a sophisticated team of fraudsters pretended to be employees and executives of Binance, one of the world's leading blockchain ecosystem and digital currency exchange platforms. These impersonations were made on social networking platforms including Twitter, LinkedIn, and Telegram messenger. The most sophisticated of these impersonations was of the company's Chief Information Officer (CIO), Patrick Hillmann. The fraudsters used TV and news interviews and appearances to create a deepfake of Mr. Hillmann and then infiltrated various company virtual meetings with the fake CIO in attendance.[25]

While the deepfake did not result in financial theft, it did raise other concerns. If a key executive can be impersonated in real time in meetings with colleagues, sensitive data could be stolen or made public including trade secrets, strategies, confidential client or employee information, and even non-public financial information.

What is a Deepfake?

A deepfake uses AI and machine learning to manipulate visual or audio content for the purpose of deception. Most commonly, this is a video of a person in which their face or body has been digitally altered so that they appear to be someone else. Face manipulation can be further categorized into the following types:

- Face replacement: Using the face of one person and placing it over the face of another.
- Face re-enactment: Manipulating the features of a target face to make it look like it is saying something that it is not.
- Face generation: Creating a convincing but fictional face that can be manipulated.
- Voice spoofing: Altering the voice of a person in real time to mimic the voice of another.[26]

Audio Deepfakes

Deepfakes go beyond just video and imagery. Audio deepfakes use AI-synthesized content to create highly realistic synthetic voices which can be combined with videos to further blur what is real. With the ability to spoof voices, audio deepfakes are being used for misinformation purposes due to their relative ease of use and the accessibility of audio editing tools.[27]

One consequence of an audio deepfake being used to perpetrate fraud occurred in 2019 when a UK-based energy firm transferred nearly 200,000 British pounds ($260,000) to a Hungarian bank account. The transfer was initiated after a call from the CEO of the UK firm's corporate parent making the request for the transfer. What was exceptional about this ordinary corporate transfer was that the CEO did not make this call. Instead, the call used AI voice mimicry software, allowing someone else to impersonate the CEO in real time. This voice spoofing was so advanced, mimicking even the subtle German accent of the CEO.[28]

How and Why Deepfakes are Used in Hiring

The FBI and Europol have issued multiple warnings on the use of deepfakes to commit fraud in the work environment. In 2022, the FBI issued a Private Industry Notification warning of the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for remote work and work-at-home positions.[29] In 2020, Europol warned of deepfakes and their potential use in securities fraud, stating "deepfakes could be instrumentalized as part of stock market manipulation or fraud schemes."[30]

Deepfakes are used in hiring to convincingly misrepresent someone as the applicant in interviews for jobs that can be performed remotely. The initial goal is to gain a position within a company which leads to access to a variety of information that can be used for illegal purposes. These fraudulent new hires can access corporate or trade secrets, competitor information, sales information including competitor bidding, financial data and customer data.

The most targeted positions are remote work and work-at-home positions, and the most targeted job sectors include information technology (IT), software development, human resources (HR), and lending. Any positions that would allow access to customers' personal information, financial data, corporate IT databases, and/or proprietary information are fraud targets.

Deeper Discussion on Synthetic Identities

As with deepfakes, synthetic content also uses AI generation and manipulation tools. But instead of mimicking an existing person, a new synthetic persona is created. The March 2021 FBI Private Industry Notification warned of synthetic content being used for cyber and foreign influence operations. While related to deepfakes, when discussing synthetic content as it relates to KYE, we will focus specifically on synthetic identities, primarily on the use of speech synthesis and face morphing.

What is a Synthetic Identity?

As with deepfakes, synthetic identities also use AI content generation and manipulation tools. The result is then combined with various Personally Identifiable Information (PII) from one or more real people to create a new, synthetic persona instead of mimicking an existing person.

The most common result is the generation of an entirely new fake profile image using a generative adversarial network (GAN). These GANs can produce highly convincing fake images of human faces.[31] There are multiple sites on the Internet that will generate these images on command. Some of the sites offer a variety of customizable options to tailor these profile images including age, sex, ethnicity, and eye color. There are even emotional options such as joy.[32]

Speech Synthesis

The creation of a synthetic identity does not just stop at imagery. Producing a voice to enhance the synthetic identity is created through speech synthesis. This is achieved using text-to-speech (TTS) or voice conversion (VS), converting normal language that is typed into an online platform into speech. Basic software is available for free or at a low cost online that balances the quality of speech synthesis through naturalness and intelligibility.

Two common offerings of speech synthesis are stock voices provided by online offerings and the creation of a unique voice that uses Deep Neural Networks (DNN) to create a voice by being trained on recorded speech.

Synthetic speech is neither good nor bad and offers many positive uses. Examples of these uses include:

- Enabling speech for those who cannot or are hindered in their ability.
- Allowing text to be read aloud to those who are hearing impaired or require more annunciated audio.
- Clearer, consistent voiceovers for videos, broadcasts, audiobooks, or other recordings.
- Recording voice for historical and entertainment purposes .
- Easier ability to have audio spoken or presented in other languages.[33]

However, like other technologies, speech synthesis can be used for harm or fraud. It can be combined with partial or complete synthetic identity background characteristics already created through a profile image, name, and other descriptive characteristics to generate a complete synthetic persona. This fake persona can be used to obtain employment.

Face Morphing

A variation of synthetic identities is the use of face morphing where two or more individuals use AI to merge their photos into the likeness of one. This results in a profile image that retains the likeness of both or all individuals with the goal of tricking human ID examiners and less advanced biometrics.

Real world threats are a result of how images created using face morphing can be used to fraudulently obtain identification documents. By submitting the generated image with identification document applications, it is possible to obtain a genuine document that can be used to further obtain additional fraudulent documents. Renewal applications may be even easier to obtain through this method as there is already an image on file that is being updated with the face-morphed image.

A fraudulent ID can also be created with the use of face morphing to obtain a printed forged ID using the morphed photo. Both uses of face morphing can in turn facilitate the ability to obtain other IDs such as birth certificates.[34]

How and Why Synthetic Identities are Used in Hiring

Synthetic identities, as with deepfakes, present a challenge to the recruitment of employees, primarily with positions that are remote or where the candidate would not initially be met in person. As discussed in the previous section on deepfakes, and earlier with identity obfuscation, synthetic identities are used to obtain positions that would allow access to a company's proprietary information. Three FBI warnings in less than two years attest to the need for a deeper authentication of each new employee to help mitigate the damage that could affect an organization with a fraudulent hire.

Deeper Discussion on Shallowfakes

We discussed deepfakes and their use of AI to alter video and audio content. A variation of deepfakes is known as shallowfakes. Shallowfakes (also known as cheap fakes) are defined by Europol as "videos or audio recordings that are either presented out of context or are doctored with simple editing tools."[35] The primary difference that distinguishes shallowfakes from deepfakes is their limited or nonexistent use of AI in their manipulation. Shallowfakes most often use simple audio or video editing tools to alter the results in a way that changes the context of the original.

How Shallowfakes are Used for Harm

One of the more notorious uses of a shallowfake was a news clip that circulated throughout the U.S. media showing the U.S. House Speaker Nancy Pelosi appearing to be drunk. The malicious intent of the video was a result of news footage of Speaker Pelosi slowed down using video editing tools just enough to infer signs of inebriation but not slow enough that a viewer would notice. The result was then released to the media with the intent to harm and discredit the Speaker.[36] Another example of a shallowfake that also gained wide media coverage was a video of a speech by John Fetterman, a candidate for the U.S. Senate in 2022. Sound was removed from audience scenes in the news footage with basic video editing tools, implying Fetterman was confused and lacked the audience's attention.[37]

How Shallowfakes are Used in Hiring

The Pelosi and Fetterman examples of shallowfakes did not use AI in their deception but are still related to deepfakes in their basic manipulation of visual and audio content. Both involved politicians and both highlighted how quickly manipulated disinformation can spread when the person faked has some level of newsworthiness.

At a minimum, shallowfakes can be used to misrepresent an employee's skills and general capabilities and overall awareness of what is needed for the employment position. With higher profile positions or employees in strategic positions, shallowfakes can be used to harm an organization or its stakeholders.

An extreme example of a shallowfake being used for theft was demonstrated in 2019 when it was revealed that a French-Israeli citizen, Gilbert Chikli, was able to steal an estimated $90 million by impersonating French defense minister Jean-Yves Le Drian. Mr. Chikli was accused of fraudulently raising funds under the guise that he was securing the release of French citizens being held by terrorists. The con utilized the lower quality of video chats and the manufacture of both a silicon mask created to look like the defense minister and a set to replicate his ministerial office. While primitive by today's AI standards, it still demonstrates the effectiveness and breadth of identity theft.[38]

Current Mitigation Measures Recommended by the U.S. Government

We have discussed current hiring practices, their limitations, and the resulting risks exposed to an organization. A brief discussion of the methods used in hiring fraud was also presented. The U.S. government and other world organizations have provided a variety of strategies and tactics that can be followed to limit exposure to hiring fraud.

Potential Mitigation Measures

In guidance issued by the U.S. Department of State, the U.S. Department of the Treasury, and the FBI, specific mitigation measures are called out when hiring a new employee.[39] Organizations are advised to:

- Closely scrutinize submitted identity verification documents for signs of forgery and reject low-quality image documents.
- Conduct a video interview to verify the identity of the applicant.
- Conduct a pre-employment background check, drug test, and create a fingerprint/biometric log-in to verify their identity and claimed geographic location.
- Verify employment and higher education history directly with the listed companies and educational institutions in an applicant's resume and online employment history profiles using contact information obtained through a search engine or business database, not from the potential employee.

Additional measures for the hiring of freelance programmers and developers:

- Regularly check how your platform is being accessed, whether through remote desktop sharing software or a VPN or VPS. This is important if VPN access is not standard practice.
- Flag all job applicants that use the same or similar document templates or project communications.
- Conduct full account verification and extra scrutiny on all newly established accounts.
- Check that all provided information including spelling, nationality, and other details is consistent with the information on the developer's freelance profiles, social media, external portfolio websites, and payment account platforms.
- Raise caution of a developer requesting to communicate on platforms outside the original freelance platform.

> ***Traditional identity verification assumes that when a person provides an ID, that ID is real and correct. Without proving an identity, the identity of the employee is only as good as the ID being used.***

We already discussed the many consequences of hiring fraud that an organization can face when a fraudulent hire gains access to an organization's private and proprietary information that can go beyond financial costs. There are additional consequences that can be quite severe if employment is offered to someone from a country that is not permitted to work in the U.S. These can include:

- Sanctions by the Department of the Treasury's Office of Foreign Assets Control (OFAC)
- Statutory penalties
- Civil monetary penalties which can be greater than applicable statutory penalties
- Restrictions on importing goods made in other countries
- Restrictions or loss of ability to clear monetary transactions in the U.S.
- Imprisonment
- Potential forfeiture of property

Identity Proofing: Going Beyond Background Checks

The preceding guidance is complicated, difficult, and may often be unreasonable for an organization and the person(s) tasked with adhering to it. Incorporating standard employment background checks will address many of the mitigation measures recommended by the U.S. government. Organizations can also opt in for enhanced background checks that will include credit checks, employment history checks, and education verifications.

Combined, these checks strengthen the thoroughness of a background check, but they all still rely on one key assumption: That the person providing an ID for these verifications is the person on that ID. Identity proofing goes further.

Identity Proofing Defined

Identity proofing confirms a person is who they say they are. Any presented ID is verified to be a correct document that has not been altered and the person presenting the document is proven to be the person on the document.

The U.S Government defines identity proofing as "the process of linking records in a database to a real-world person." They also provide standards to be followed for the process of identity proofing.[40]

What is the difference between identity proofing and verifying an identity?

Traditional identity verification assumes that when a person provides an ID, that ID is real and correct. IDs such as a driver's license, social security card, or birth certificate can be verified and deemed authentic, providing verification of the identity on the document. But this does not prove the person who presents the document is the person on the document. Identity proofing goes beyond traditional ID verification to prove who a person actually is. Without proving an identity, the identity of the employee is only as good as the ID being used.

NIST Framework for Identity Proofing

The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, developed a framework for identity proofing that involves identity resolution, identity evidence collection and validation, and identity evidence quality. Per the NIST, "the requirements are intended to ensure the claimed identity is the actual identity of the subject attempting to enroll with the Credential Service Provider (CSP) and that scalable attacks affecting a large population of enrolled individuals require greater time and cost than the value of the resources the system is protecting."[41]

One of the challenges with digital identity is the ability to associate a specific person with their activities, whether online or through system access. The concept of identity proofing was created to resolve this challenge. With identity proofing, an individual goes through an enrollment process where evidence of their identity is collected, validated, and verified.

Following is an example of what the process entails:

Resolution (collection): PII is collected from the applicant including name, address, date of birth. Multiple forms of identity are also collected such as a passport and driver's license.

Validation: The information supplied is validated through an authoritative source. This will include content on the ID, along with confirming the provided evidence was not affected.

Verification: The applicant is verified visually to the provided ID such as comparing a selfie to a photo on a driver's license.

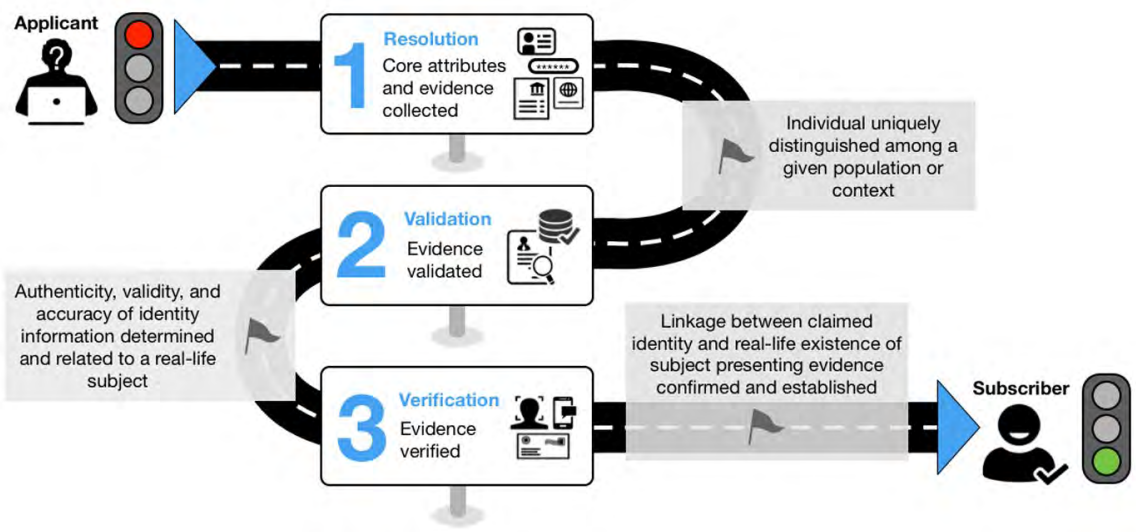


Diagram: The Identity Proofing User Journey. NIST Special Publication 800-63A.

The NIST developed three levels of identity assurance:

IAL1: The applicant's identity is not required to be proven. Any self-asserted attributes are neither validated nor verified.

IAL2: Evidence is required and verified to support the existence of the claimed identity and must be verified either remotely or in person. The collection of biometrics is optional for verification.

IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative. The collection of biometrics is mandatory for identity proofing.

The Credential Service Provider (CSP) is the organization conducting the identity proofing process. It is responsible for establishing and maintaining the enrollment records and building authenticators to the enrollment records. The sole objective of identity proofing is ensuring that an applicant is who they claim to be to a stated level of certitude, so the CSPs must collect, validate, and verify the minimum attributes necessary to accomplish identity proofing. The CSP will choose the level of identity assurance that balances the levels of friction in obtaining identity evidence, the privacy of the person being verified, and the minimum level of identity proofing assurance an organization is comfortable with.[42]

Identity Proofing and KYE by Q5id

We followed our overview of current fraudulent methods being used to obtain employment, by listing two paths an organization can follow to limit exposure to the results of hiring fraud.

Path 1 is to follow government recommended mitigation measures. These include scrutinizing any identity verification documents, conducting video interviews, managing background and education checks, and verifying their employment history.

Path 2 is to implement an identity proofing strategy that goes beyond ID verification by proving any new hire is who they say they are.

KYE by Q5id

KYE by Q5id believes only Path 2 will provide an organization with the assurance that their employee is who they say they are. Q5id's solution uses our patented IP to create a Q5id Proven Identity. We do this in a two-step process that meets and exceeds NIST IAL2 standards (and NIST IAL3 standards when opting for our remote identity proofing using an authorized and trained representative for the identity proofing process).

Step 1:

We identify the individual as a unique person through our verification process. This process includes an enhanced vetting of the identification provided by the employee and then verifying that the identification has not been tampered with and that the information on the provided ID is correct. This can include verifying specific ID attributes such as the name, birthday, and ID number. We then take each attribute and prove them. This will include verifying the ID is not forged and verifying the picture on the license is the person presenting the document.

Step 2:

With AI, we use multiple biometrics to test for liveness and deepfakes and to verify the image on the identification matches the facial biometrics. By associating the verified attributes to the person, we then associate the biometrics to these attributes in Step 1, creating a Q5id Proven Identity of which a duplicate proven identity cannot be created with the same biometrics. The biometrics used for the proven identity uses a hashing algorithm, and the face and palm biometrics are converted into a character string that cannot be reverse engineered.

FAR and Our Level of Accuracy

A proven identity must be accurate to a level of accuracy that far surpasses any acceptable level of incorrectness, to allow it to be relied on by any party needing a true ID verification. KYE by Q5id measures this level of accuracy through use of FAR.

As defined in Webopedia, "False Acceptance Rate (FAR) is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts."[43] [31]

As a result of our identity proofing process that incorporates our patented IP, we calculated our FAR as 1 in 933 billion or 0.00000000011%. Or put even more simply, we would not find a duplicate person until we verified 933 billion people, or 116 times the population of Earth.

We derived this calculation from three of our methods used in generating a proven identity.

1. Face recognition provides a 0.00021% (1 in 466,666) of multiple system identities.
2. Face liveness provides a 0.15% (1 in 667) of multiple system identities.
3. Palm Recognition provides a 0.00005% (1 in 20,000,000) of multiple system identities.

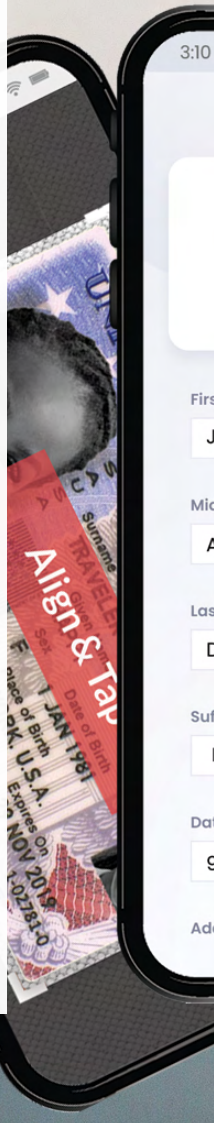
Combined, these three methods alone provide our FAR.

Conclusion

All companies with U.S. employees must verify the identity of the person they are hiring by requesting and examining one or two identification documents, as required by Form I-9. Companies can go further in their employee verification process by requesting additional checks, including background, credit, and education checks. But with the continued advancement of technology, there is a corresponding growth in hiring fraud, especially among remote and work-from-home workers. The use of artificial intelligence, video and audio editing tools, and the relative ease of accessing the personal information of other people are all being used to wrongfully gain employment.

Employers now must be aware of stolen identities, deepfakes, synthetic identities, and even the obfuscating of one's true identity with their job applicants. New hires, including those hired through fraudulent means, gain access to an organization's proprietary information. Despite warnings from multiple government agencies along with recommended measures to help mitigate the wrongful hiring of employees, there is a need for further methods for identity verification.

Know Your Employee (KYE) is an improvement on the current employee verification process by proving each job candidate is who they say they are. KYE by Q5id goes beyond NIST IAL2 requirements by incorporating multiple biometrics into our identity proofing process. We also incorporate liveness testing into our patented solution to provide a FAR of 1 in 933 billion. With the continuous advancement and new techniques in identity theft, organizations need to also stay adept in the way they verify their new employees. KYE by Q5id was created to detect employee identity fraud in today's hiring environment, giving employers the level of assurance needed to know exactly who their employees are.




Bio Verification
Does this look correct?
Complete the form. You can edit any out of date information.
3:08
Capturing...
Natural light
No glare

Glossary

Audio Deepfakes: A subset of deepfakes that use AI-synthesized content to create highly realistic synthetic voices which can be combined with videos.

CSP: Stands for Credential Service Provider. The CSP is the organization conducting the identity proofing process and is responsible for establishing and maintaining the enrollment records and building authenticators to the enrollment records.

Deepfakes: A deepfake uses AI and machine learning to manipulate visual or audio content for the purpose of deception. Most commonly, this is a video of a person in which their face or body has been digitally altered so that they appear to be someone else.

FAR: Stands for False Acceptance Rate and is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

Face Morphing: A variation of synthetic identities where the faces of two or more individuals using AI are merged into the likeness of one, resulting in a profile image that retains the likeness of both or all individuals. Often with the goal of tricking human ID examiners and less advanced biometrics.

Form I-9: A U.S. Government form which is used to verify the identity and employment authorization of individuals hired for employment in the United States.

Identity Obfuscation: Deliberately obscuring one's identity. This can include one's location and nationality, often using other names as aliases.

Identity Proofing: Confirms a person is who they say they are through a process of linking records in a database to a real-world person. The United States Government provides a set of standards for identity proofing through the NIST Special Publication 800-63.

KYC: Stands for Know Your Customer and is a requirement that the financial services industry uses to obtain basic information about their clients. This information includes at a minimum the client's name, date of birth, address, age, and taxpayer ID.

KYE: Stands for Know Your Employee and is process of proving the identity of an employee.

NIST: Stands for National Institute of Standards and Technology and is part of the U.S. Government. They developed security and privacy controls for digital identity management published as NIST SP 800-63. This publication provides technical requirements for implementing digital identity services.

PII: Stands for personally identifiable information. This can include a person's name, address, and date of birth.

Shallowfakes: Also known as cheap fakes, shallowfakes are videos or audio recordings that are either presented out of context or are doctored with simple editing tools to misrepresent what the actual media presents.

Speech Synthesis: The production of a voice used to enhance a synthetic identity or to be used on its own. Most commonly achieved using text-to-speech (TTS) or voice conversion (VS), converting normal language that is typed into an online platform into speech.

Stolen Identity: The most common form of identity theft and usually involves the theft of personal information such as the name, social security number, and date of birth. This information is then used to present themselves as that person to commit fraud.

Synthetic Identity: False identity made using AI content generation and manipulation tools along with various Personally Identifiable Information (PII) from one or more real people that are combined to create a new, synthetic persona.

Bibliography

1. Association of Certified Fraud Examiners, Inc. (2022). Occupational Fraud 2022: A Report to the Nations. https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

2. Glassdoor Team. (2019, July 5). How to calculate cost-per-hire. Glassdoor. https://www.glassdoor.com/employers/blog/calculate-cost-per-hire/

3. Smith, Z., & Lostri, E. (2020, December). The Hidden Costs of Cybercrime. McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

4. IBM. IBM Security & Ponemon Institute, LLC. (2022, July). Cost of a Data Breach Report 2022. IBM. https://www.aba.com/-/media/documents/reports-and-surveys/aba-ow-trusted-digital-identities-nov-2022.pdf?rev=60dbac8bd0c6446a8e843908d394266f

5. U.S. Citizenship and Immigration Services. (Accessed 2022, November 18). I-9, Employment Eligibility Verification. https://www.uscis.gov/i-9

6. Association of Certified Fraud Examiners, Inc. (2022). Occupational Fraud 2022: A Report to the Nations. https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

7. Chang, J. (2022, November 11). 119 Impressive Cybersecurity Statistics: 2021/2022 Data & Market Analysis. FinancesOnline. https://financesonline.com/cybersecurity-statistics/

8. Federal Bureau of Investigation. (2022, June 28). Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions [Public Service Announcement]. https://www.ic3.gov/Media/Y2022/PSA220628

9. Federal Bureau of Investigation. (2021, March 10). Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations [Public Service Announcement]. https://www.ic3.gov/Media/News/2021/210310-2.pdf

10. Nimmo, B., Agranovich, D., & Gleicher, N. (2022). Adversarial Threat Report. Meta. https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf

11. Federal Bureau of Investigation. (2021, March 10). Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations [Public Service Announcement]. https://www.ic3.gov/Media/News/2021/210310-2.pdf

12. St. James, Emily. (2014, March 5). Mad Men: “Nixon Vs. Kennedy”. AV Club. https://www.avclub.com/mad-men-nixon-vs-kennedy-1798179680

13. United States Government Accountability Office. (2022, May). Employment Related Identity Fraud: Improved Collaboration and Other Actions Would Help IRS and SSA Address Risks (GAO-20-492). https://www.gao.gov/assets/gao-20-492.pdf

14. U.S. Department of State, U.S. Department of the Treasury, & Federal Bureau of Investigation. (2022, May 16). Guidance on the Democratic People’s Republic of Korea information technology workers. https://home.treasury.gov/system/files/126/20220516_dprk_it_worker_advisory.pdf

15. Federal Bureau of Investigation. (2022, June 28). Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions [Public Service Announcement]. https://www.ic3.gov/Media/Y2022/PSA220628

16. Ryan, C. (2021, January 18). Solving the Fraud Problem: What is Synthetic Identity Fraud? Experian. https://www.experian.com/blogs/insights/2021/01/solving-fraud-problem-synthetic-identity-fraud/

17. European Union Agency for Law Enforcement Cooperation. (2020). Malicious Uses and Abuses of Artificial Intelligence. https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

18. United States Government Accountability Office. (2022, May). Employment Related Identity Fraud: Improved Collaboration and Other Actions Would Help IRS and SSA Address Risks (GAO-20-492). https://www.gao.gov/assets/gao-20-492.pdf

19. National Council on Identity Theft Protection. (Accessed 2022, November 22). What is Employment Identity Theft and How Can it Occur? https://identitytheft.org/types/employment/

20. U.S. Department of State, U.S. Department of the Treasury, & Federal Bureau of Investigation. (2022, May 16). Guidance on the Democratic People’s Republic of Korea information technology workers. https://home.treasury.gov/system/files/126/20220516_dprk_it_worker_advisory.pdf

21. The Free Dictionary. (accessed 2022, November 22). Farlex. https://www.thefreedictionary.com/obfuscation

22. Goodwin, P. (2020, March). Identity obfuscation through the exchange of keystroke biometric data. [Thesis, Naval Postgraduate School]. https://apps.dtic.mil/sti/pdfs/AD1114215.pdf

23. U.S. Department of State, U.S. Department of the Treasury, & Federal Bureau of Investigation. (2022, May 16). Guidance on the Democratic People's Republic of Korea information technology workers. https://home.treasury.gov/system/files/126/20220516_dprk_it_worker_advisory.pdf

24. U.S. Department of State, U.S. Department of the Treasury, & Federal Bureau of Investigation. (2022, May 16). Guidance on the Democratic People's Republic of Korea information technology workers. https://home.treasury.gov/system/files/126/20220516_dprk_it_worker_advisory.pdf

25. Hillman, P. (2022, August 17). Scammers Created an AI Hologram of Me to Scam Unsuspecting Projects. Binance. https://www.binance.com/en/blog/community/scammers-created-an-ai-hologram-of-me-to-scam-unsuspecting-projects-6406050849026267209

26. European Union Agency for Law Enforcement Cooperation. (2020). Malicious Uses and Abuses of Artificial Intelligence. https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

27. Lyu, Siwei. Computer Science Department, University at Albany, State University of New York. DeepFake Detection: Current Challenges and Next Steps. https://www.arxiv-vanity.com/papers/2003.09234/

28. Damiani, J. (2019, September 3). A Voice Deepfake Was Used To Scam A CEO Out Of $243,000. Forbes. https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=e279021224

29. Federal Bureau of Investigation. (2022, June 28). Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions [Public Service Announcement]. https://www.ic3.gov/Media/Y2022/PSA220628

30. European Union Agency for Law Enforcement Cooperation. (2020). Malicious Uses and Abuses of Artificial Intelligence. https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

31. Peng, T. (2018, December 14). GAN 2.0: NVIDIA's Hyperrealistic Face Generator. Synced. https://syncedreview.com/2018/12/14/gan-2-0-nvidias-hyperrealistic-face-generator/

32. Generated Photos. (Accessed 2022, November 18). https://generated.photos/faces

33. Veritone. (Accessed 2022, November 23). Deepfake Voice: How AI companies are tackling deepfake voice fraud. https://www.veritone.com/blog/how-ai-companies-are-tackling-deepfake-voice-fraud/

34. European Union Agency for Law Enforcement Cooperation. (2020). Malicious Uses and Abuses of Artificial Intelligence. https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

35. European Union Agency for Law Enforcement Cooperation. (2020). Malicious Uses and Abuses of Artificial Intelligence. https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

36. Harwell, D. (2019, May 24). Faked Pelosi videos, slowed to make her appear drunk, spread across social media. Washington Post. https://www.washingtonpost.com/technology/2019/05/23/faked-pelosi-videos-slowed-make-her-appear-drunk-spread-across-social-media/

37. Kaonga, G. (2022, September 16). John Fetterman Speech Fuels Controversy Amid 'Doctored Video' Claims. Newsweek. https://www.newsweek.com/john-fetterman-fact-check-viral-video-speech-update-latest-stroke-dr-oz-1743248

38. El-Ghobashy, T. (2019, June 20). How scammers used a silicone mask and Skype to impersonate a French minister and steal $90 million. Washington Post. https://www.washingtonpost.com/world/how-scammers-used-a-silicone-mask-and-skype-to-impersonate-a-french-minister-and-steal-90-million/2019/06/20/601ca6ac-9375-11e9-b72d-d56510fa753e_story.html

39. U.S. Department of State, U.S. Department of the Treasury, & Federal Bureau of Investigation. (2022, May 16). Guidance on the Democratic People's Republic of Korea information technology workers. https://home.treasury.gov/system/files/126/20220516_dprk_it_worker_advisory.pdf

40. Strategic & Research. (2017). Identity In A Digital Age: Infrastructure For Inclusive Development. USAID. https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

41. Grassi, P., & Fenton, J. National Institute of Standards and Technology. (2017, June). Digital Identity Guidelines: Enrollment and Identity Proofing (Publication No. 800-63A). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

42. Strategic & Research. (2017). Identity In A Digital Age: Infrastructure For Inclusive Development. USAID. https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

43. Beal, V. (2004, April 6). False Acceptance. Webopedia. https://www.webopedia.com/definitions/false-acceptance

Q5id

The Patented Proven
Identity Solution

(855) 438-7543

q5id.com