Impersonation of government entities could cost more than $800 million in losses this year

Identity related scams generated more than $20 billion in losses in 2024, with more than 22 million victims. This figure is set to increase by 2025 due to the sophistication of technology, especially deepfakes and the use of AI.

Between May 2023 and the same month this year, there were more than 6,300 breaches of the integrity of databases containing users' personal information that can be used to impersonate public or financial institutions.

Identy.io's biometric identity verification solutions provide users a layer of security to minimise the possibility of fraud and identity theft when dealing with public administrations thanks to security measures such as passive liveness that make it virtually impossible to forge an identity, even using artificial intelligence models or silicon fingerprint replicas.

Impersonation continues to represent significant losses for American society. A problem that, according to data from the Internal Revenue Service (IRS) of the country, increased in 2024 by 171 million dollars compared to the previous year, and that in 2025 could exceed 800 million. The theft of personal information, such as Social Security numbers, or financial data, can be used to perpetrate tax fraud of all kinds. In total, according to the Federal Trade Commission (FTC), in 2024 fraud or identity theft-related scams accounted for losses of more than $20 billion, with more than 22 million victims recorded nationwide. A figure that, presumably, will increase in 2025 due to the sophistication of technology, especially deepfakes and the use of AI.

For this reason, Identy.io, international leading company of biometric and digital credential management solutions, has incorporated into its touchless biometric verification solutions with liveness passive all the technical innovations available to meet the highest security standards in the market, so as to ensure that those digital procedures that are carried out guarantee that the user who carries out the transaction is who really claims to be.

In addition to identity theft problem, in the period between May 2023 and the same month this year, the US Identity Theft Resource Center (ITCR) has recorded more than 6,300 attacks and compromises to the integrity of databases with personal and financial information of US citizens, including the one suffered by Change Healthcare in 2024, with information on more than 190 million users compromised. Therefore, faced with the growing risk of fraud and identity theft, it is essential to ensure that the digital transactions carried out with public and governmental entities, but also with financial institutions, have the highest guarantees of security and protection.

Identy.io's identity verification solutions use passive liveness detection technology to minimize as much as possible the possibility of identity theft. This technology analyzes certain physical characteristics of the user, such as facial movements in the case of face verification solutions, without requiring the user to perform any specific movement or action. This technology not only makes identity verification more accessible to anyone, regardless of their background or technological knowledge, but also makes it virtually impossible to impersonate, as it is able to detect and discard any attempt to access the user's digital credentials, even in cases where a deepfake or silicon fingerprint replica is used.

As a way to ensure that no leakage or identity theft occurs in such transactions, Identy.io's solutions process all the user's information from their own mobile phone, unlike other solutions available in the market. Once the user completes the onboarding process, in which it is verified that the captured biometric information really belongs to the user, a digital identity credential is generated and stored in the user's terminal under encryption, so that no queries to any external server or cloud service are necessary, minimising the risks related to identity theft.

In the same way, the user can decide at any time what personal information to share depending on the procedures or formalities they want to carry out, thus preventing third parties from having access to data that may not be relevant at the time. Thus, Identy.io's solutions are confirmed as allies for the user in their security, but also for public entities, which reduce the chances of suffering fraud of all kinds. These frauds can affect the completion of official procedures, such as tax proceedings with the IRS - filing tax returns or accessing accounts online -, applications for Social Security benefits or unemployment benefits, immigration procedures or those related to obtaining driving licences, passports or false birth certificates.

According to Jesús Aragón, CEO of Identy.io, ‘we applaud the efforts of the government and public entities to reduce the risks of fraud in the digital procedures carried out by millions of users every day thanks to the implementation of measures such as passkeys. However, we believe that it is necessary to go further, and that only biometric touchless verification solutions with passive liveness are the answer to this social scourge. By reducing the risk of duplicating a user's identity to virtually zero, solutions such as those offered by Identy.io can help save billions of dollars for users and public entities’.

Identy.io's solutions offer users a secure and easy-to-use interface, and in turn, contribute to increase efficiency and profitability in their use for public and private entities that implement them, as they do not require costly investments in third-party infrastructure or cloud management to store and manage users' digital credentials. They also meet the highest security standards, such as those proposed by the US NIST (National Institute of Standards and Technology), by supporting eKYC (Know Your Customer Digitally) processes and AML (anti-money laundering) frameworks, as well as complying with the ISO 30107-3 standard on liveness, which guarantees the security and accuracy of its portfolio of biometric identity management applications.

About Identy.io

Headquartered in the US with offices in Brazil, Mexico, Spain and India, Identy.io is the global reference in digital identity verification using touchless mobile biometrics. At Identy.io we believe in multi-factor authentication, while advocating the need to replace traditional methods of identity verification using passwords, tokens or OTPs (One Time Passwords), which do not guarantee the user's identity.

At Identy.io we work with institutions to secure identity in their business processes by using touchless biometrics from users' mobile devices. Our liveness authentication protection makes biometrics secure and deployable on a large scale. For more information, visit https://identy.io