Using Biometric Technology To Fight Public Sector Benefit Fraud

Protecting American Society's Most Vulnerable from Generative AI Crime

Introduction

The pandemic caused a scramble to digitize typically in-person services to provide extensive financial aid to those in need. Unfortunately, because of the critical nature of the situation, remote access to benefits was launched before federal and state government agencies had adequate time to ensure that these transactions would meet desired security standards.

Criminals seized the opportunity to defraud these hastily launched benefits programs, either by compromising existing accounts or remotely onboarding fraudulent identities – many of which remain in use today.

This new wave of fraudsters utilize sophisticated generative AI technologies, such as deepfakes, digitally injected attacks, and synthetic identities to undermine the government benefits programs and siphon funds away from those in need.

Defrauding government benefits programs has become a humanitarian issue whereby well-intended funds are consistently lost to bad actors – and the scale is staggering. Without a more risk-based approach, the levels of criminal activity focused on defrauding humanitarian aid programs will only increase. Pandora's box has been opened, as criminals are now equipped with the technology and tools to systematically plunder public sector benefits at scale.

With the advent of generative AI based technologies, many traditional security methods are unable to counter the scale and complexity of modern fraud. Traditional security measures that rely on something you have – like a token – or something you know – like a password – have become easy to circumvent by cybercriminals. As a result, they can no longer ensure that someone is who they claim to be remotely.

Advanced, science-driven technologies, such as biometric verification – sometimes referred to as identity proofing – can ensure that digital services and benefits are delivered to those whom they are intended to help because they are based on something you are.

In this report, we'll examine the issue of public sector benefit fraud in the US in more detail and lay out a proposed vision for technology-driven response.

Biden's State Of Union Address Sets the Tone for Public Sector Benefit Fraud Response in 2023

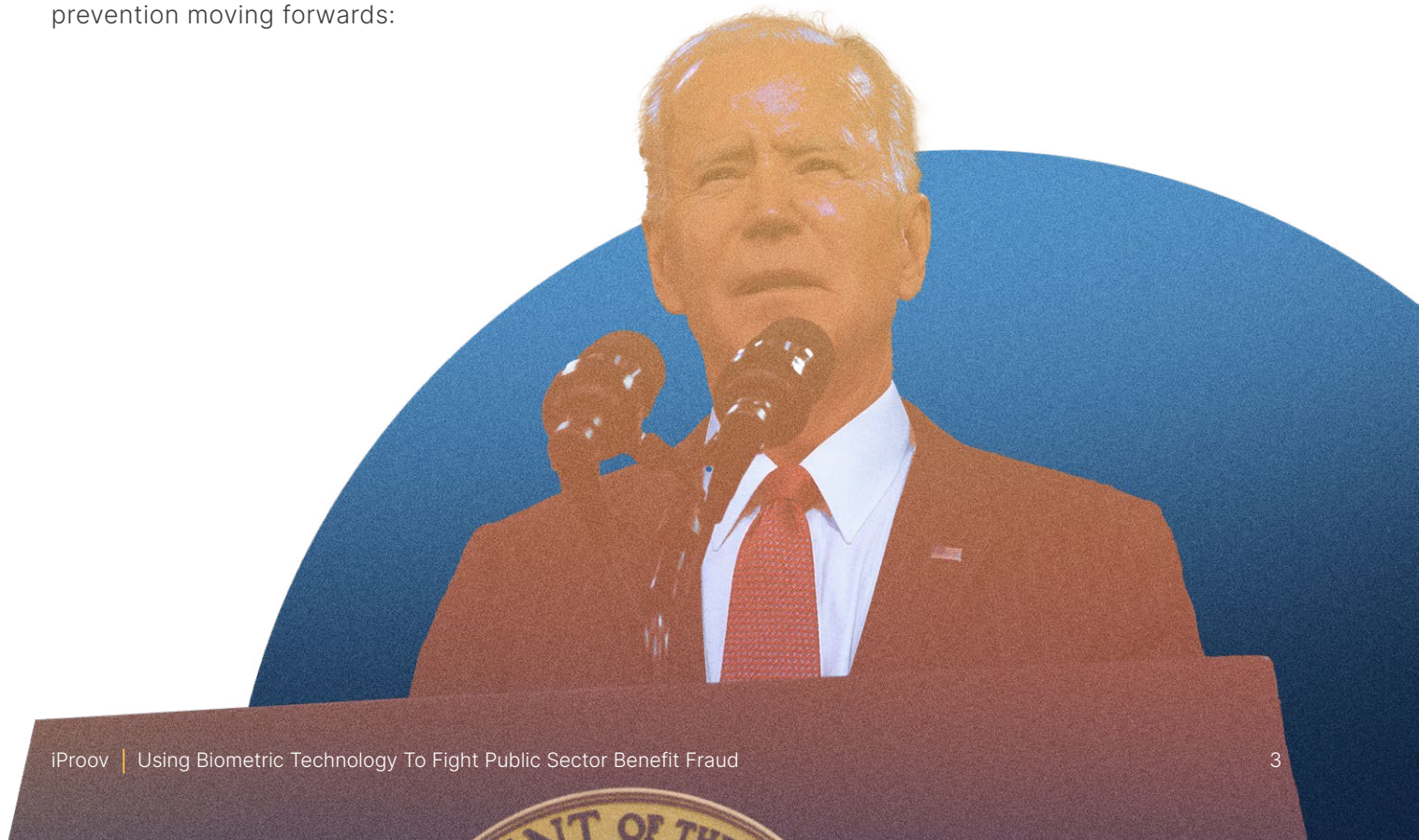
The humanitarian crisis of public sector benefit fraud has not gone unnoticed. In February 2023's State of the Union Address, Biden articulated:

"Past underinvestment in basic government technology and the crush of demand during the pandemic, combined with ill-considered decisions to take down basic fraud controls at the onset of the pandemic led to a historic degree of outright fraud and identity theft of emergency benefits."

Crucially, Biden highlighted the need for prevention moving forwards:

"The data shows that for every dollar we put into fighting fraud, the taxpayers get back at least 10 times as much. It matters."

Recovering funds in response to growing fraud creates a vicious cycle without addressing the root of the problem. Placing an emphasis on prevention by leveraging advanced technologies will be essential in curbing public sector benefit fraud at this critical juncture.



Why Does Public Sector Benefit Fraud Matter?

There's a growing sentiment that fraud is an inevitable by-product of governmental aid. Significant levels of fraud, however, should not be accepted when it is to the detriment of those who are most in need of government relief.

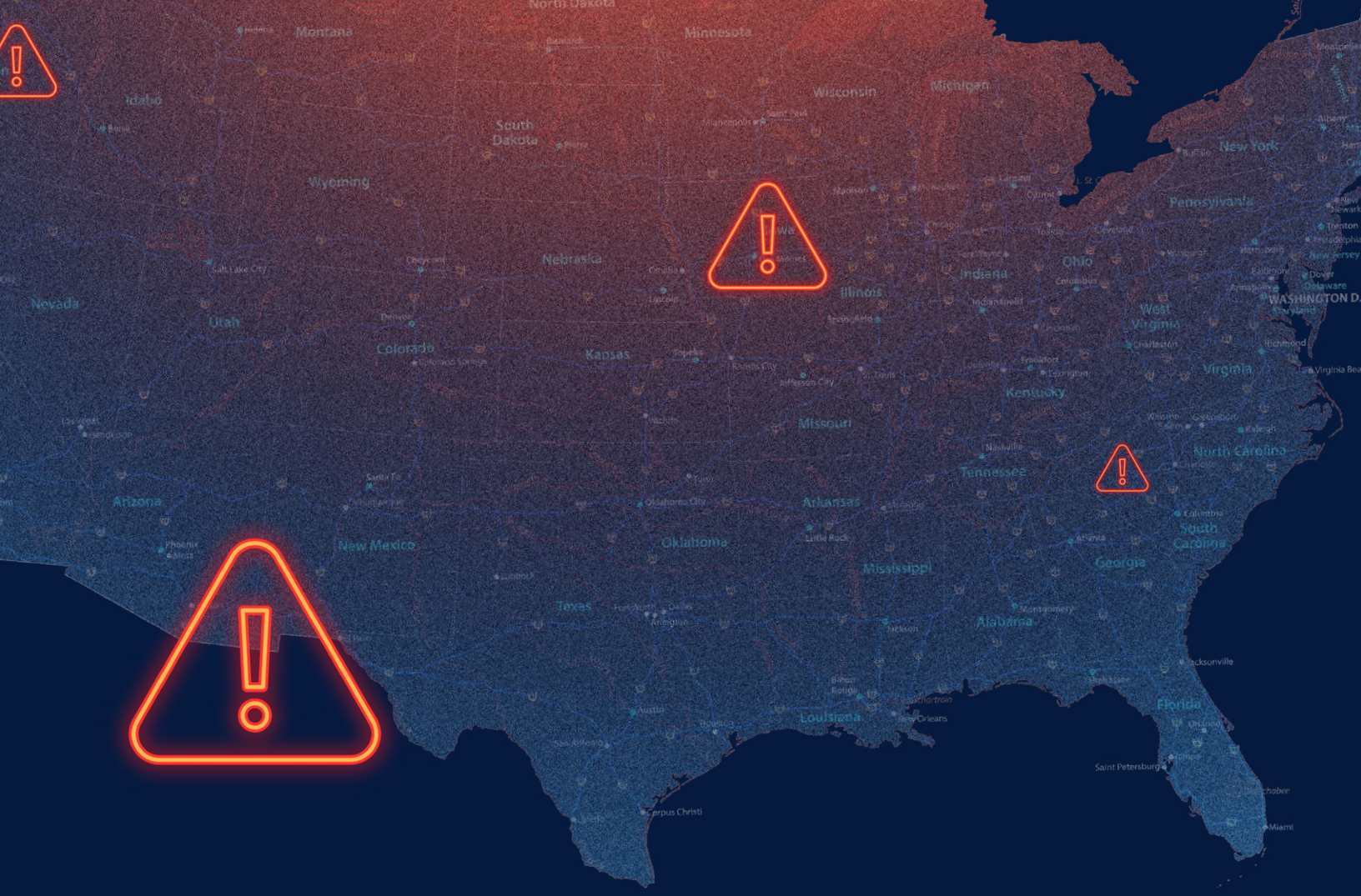
Let's consider a few impacts:

- **Americans are left without support:** Those who need aid the most find that their lifeline has been severed. More than 42 million Americans rely on Electronic Benefit Transfer (EBT) cards for everyday necessities and nutrition. But in many cases of EBT fraud, individuals find that their account has been emptied – criminals drain cards over short periods of time, generally through account takeover fraud.

- **Taxpayer money is wasted or spent inefficiently:** Money is going to fraudsters rather than those who need it most, making a mockery of the entire benefits system. A hit to the governmental budget from fraud is a hit to the level of services and care states and agencies can offer, and money saved from stemming fraud could mean billions more available to help.

- **Overspending and misdirection of funds:** The government has to spend more and more on the benefits system because it is not working as intended.

- **Fraud negatively impacts the United States' image:** When controls are not in place to curtail fraud and funds meant for public services fall into the hands of bad actors and criminal organizations, this undermines trust in the government and damages the optics of future attempts to help society's most vulnerable.



How Impactful Was Covid-19 on Public Sector Benefit Fraud?

Experts estimate that as much as $80 billion — or about 10 percent — of the $800 billion handed out in a COVID relief plan known as the Paycheck Protection Program (PPP) was stolen by fraudsters. And that's just the losses from one specific plan – not public sector benefit fraud as a whole. Similarly, Federal officials state that $191 billion in COVID aid may have been misspent solely on unemployment support.

The Department of Labor (DOL), says that one COVID-19 watchdog reported a six-times-increase in unemployment fraud investigations over pre-pandemic levels.

How Does This Compare to Traditional Fraud?

In its 2021 audit report, the Government Accountability Office found that more than $662 billion was lost due to fraud and improper payments. This figure is not contained entirely to public sector fraud alone, but gives an idea of the immense scale.

Fraud is often mistakenly thought of a victimless crime, but behind each case there's a social and psychological impact and individual story. 1 in 20, or 42 million Americans, were directly impacted by identity fraud alone in 2021. Additionally, the Federal Reserve and other agencies have been very public in stating that identity fraud is often used to fund nation-state projects in direct conflict with humanitarian programs like terrorism.

Painting a pinpoint-accurate picture of fraud is difficult due to the nature of categorization, underreporting, and the amount of fraud that goes entirely unnoticed. Its deceptive nature can make it hard to detect – successful fraud goes unnoticed. The true extent of public sector fraud remains unknown. However, these statistics begin to portray the scope of what the government is facing.

US Public Sector Benefit Fraud Case Studies: How are Fraudsters Getting Away With It?

The US Attorney's Office documents key fraud cases in online press releases. Cases are consistently and directly attributed to stolen identities, synthetic identities, and account takeover fraud.

In one shocking data point, the Southern District of Florida's U.S. Attorney's Office charged 23 separate Covid-19 relief fraud cases, with scheme amounts totaling over $150 million over the space of just a few weeks in 2022.

Let's consider a few choice examples:

Case Study 1 – Paycheck Protection Program Fraud in New York:

PPP was a huge small business covid relief package, costing $800bn. Businesses could claim money to cover 8 weeks of payroll and other business expenses. So what went wrong? Large loan sizes (max $10m) and lax application vetting standards made it a target for fraudsters. In this case, a man named Adam Arena and a group of other fraudsters defrauded the program out of nearly $1m. They spent the loans on two vehicles, spa services, clothing, restaurant meals and gym memberships. They created the synthetic identities using Social Security numbers of children, recent immigrants, the deceased, older adults and people in prison. They await sentencing.

Case Study 2 – Unemployment Fraud in Nevada:

Three men – Montes, Rivera, and Stincer – were charged in a conspiracy to apply for and use Nevada and California unemployment insurance benefit debit cards. The men used stolen Personally Identifiable Information (PII) to sign up for unemployment and had the unemployment insurance debit cards sent to mailing addresses defendants had access to. The total implicated cost was $1,149,250.

One key driver of public sector fraud is that millions of Americans' PII has already been exposed in past data breaches. This means that fraudsters have a head start in leveraging attacks against public sector systems by utilizing existing data, which can be combined with sophisticated technologies to power dangerous, scalable threats like credential stuffing attacks.

That's why remote identity verification for online services is essential – you cannot trust the integrity of the data itself. In both our case studies above, resilient biometric-enabled identity verification could have flagged that the purported identities of fraudsters' applications did not match their face when they went to apply for the benefits before the funds were released.

Additionally, advanced biometric technology can detect attempted proofing of synthetic identities, which can easily fall under the radar of traditional security checks.

The Hydra's Head: Why Attacking The Symptoms Isn't Sustainable

Today's criminals are constantly innovating to find new opportunities to infiltrate security systems. These vectors are significantly increasing the scalability and danger of threats upon public sector systems.

Organized crime networks and nation-state actors are engaging in large-scale fraud using sophisticated and evolving technologies – which the Biden administration has explicitly categorized as a major concern.

The money at stake has also encouraged the prevalence of crime-as-a-service networks. Cybercriminals develop advanced fraud tools and services and then either sell them or share the technology across criminal networks, helping criminals to learn from, test, and spread their attacks.

The scale means manual intervention is inadequate in the wider war waged against fraudsters – new heads will just keep growing back. The problem needs to be addressed at the first point of contact, when people go to sign up for access to public sector services in the first place. This is the point of highest risk – when an individual is granted access to the system and initially verifies their identity.

Using advanced technology to securely verify identity and ensure that the individual is the live, genuine human being that they claim to be is essential. It's the equivalent to cauterizing the hydra's head with fire so that nothing can grow from its neck.

A Vision for Mitigating Public Sector Benefit Fraud: Biometric Face Verification

We've established the scope, scale, and transformative nature of public sector fraud. We've established that you cannot hope to sustainably stem it reactively.

The answer lies in a solution that can prevent bad actors entering public systems at the earliest stage possible and authenticates users on an ongoing basis to ensure they are legitimate.

Accordingly, face verification has emerged as the most secure and convenient method for organizations to verify and authenticate user identity online – it's able to deliver national-grade security without compromising individual convenience when signing up for public sector benefits and services.

The face is essential because it facilitates matching a unique biometric characteristic against a trusted identity document (such as a driver's license) in order to establish genuine identity. Meanwhile, robust liveness technology works to ensure an online user is a real person, detecting if the face being presented to the camera is a live human being

Investments in advanced, science-driven fraud technology for detection and prevention, such as biometric face verification, can deliver huge payoffs – typically 10 to 100 times ROI.

Choosing a Biometric Solution for Combatting Public Sector Fraud

However, not all solutions are created equal.

Because the payoff is so big for criminals, they're going to invest huge amounts to defraud public sector systems, and they'll have access to the most sophisticated technologies. So the technology responsible for stopping them must adhere to a number of key principles if it is to ensure ongoing success:

1) A future-proofed approach to security:

- Many biometric technology providers offer some level of Presentation Attack Detection, but a comprehensive solution must also protect against more sophisticated attack methodologies. One of the most scalable and dangerous types of attacks criminals use to undermine systems today is the digital injection attack. Many biometric systems are not equipped to defend against this threat type – which is a serious problem.

- You can read more about how iProov has witnessed the threat landscape evolving dramatically and how we ensure ongoing security through real-time intelligence in our Biometric Threat Intelligence Report.

2) Cloud-based architecture:

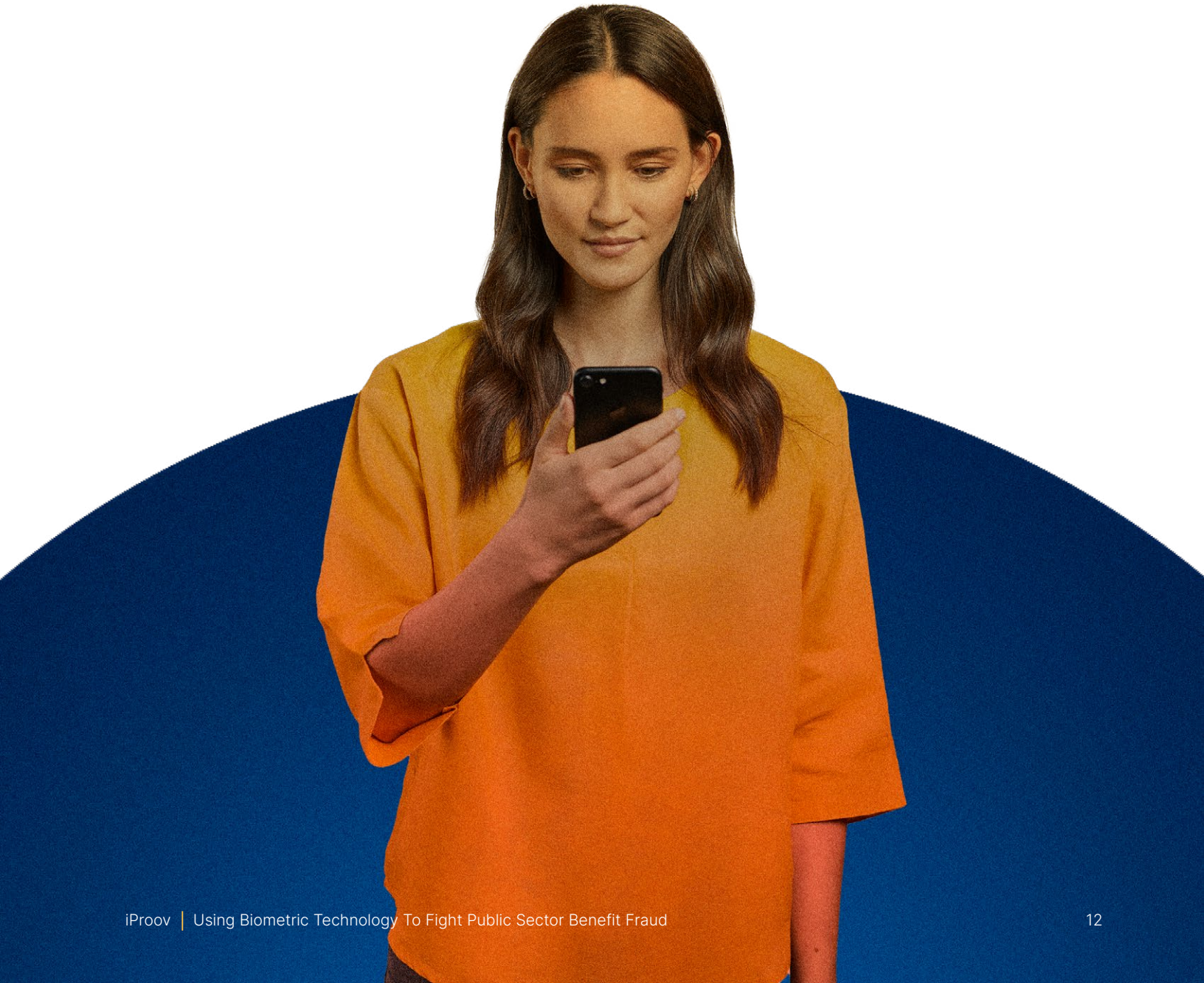
- In a 2021 Executive Order, Biden expressed support for cloud-based architecture, mandating that agency heads show how they will "prioritize resources for the adoption and use of cloud technology."

- There are many benefits to cloud-based security. First and foremost, the cloud circumvents the vulnerabilities associated with devices because authentication happens server-side, independently from the device. This means that a device affected by malware, for example, will not compromise the authentication process.

- Once a criminal has a device they can then gain access to the passwords stored on within and change the credentials – as in the case of Reyhan Ayas, who was locked out of her Apple account minutes after her iPhone was stolen and had $10,000 stolen immediately from her bank account. Similar risk applies to public sector service accounts if a device is compromised.

3) Maximum completion rates:

- How many users actually pass the biometric verification process? Factors such as device accessibility and user experience significantly impact completion rates. Even a marginal increase in fail rate is multiplied by millions of users in production, which becomes a truly significant figure. Given the USA's population, a difference of just 1% in a solution's completion rate could mean **3.3 million** people excluded from verifying their identity. Inclusivity and technological barriers to receiving aid are unacceptable.
For reference, iProov delivers industry leading completion rates (>98%).



Why Do Inclusivity and Equity Matter For Public Sector Fraud Solutions?

Additionally, the solution must provide equal access to as many people as possible. North American governments are acutely aware of the risk **of excluding marginalized communities in digital identity solutions.**

There are a number of considerations surrounding inclusivity: digital literacy, internet access, device types, accessibility concerns, biometric bias, and more. Ensure that the solution you choose has a user-centric design at its core.

The solution should:

- **Comply to WCAG 2.1 and Section 508:** WGAC guidelines assess online accessibility, and compliance ensures that the widest possible audience and avoid excluding citizens and customers from accessing digital services.
- **Be device and platform-agnostic:** Does the solution require specialist hardware or expensive technology? If so, you've already excluded a number of individuals from the process.
- **Provide passive rather than active authentication:** Reading complex instructions or performative actions is a no-go. Technology should do the work.
- **Combat bias in systems:** Diverse datasets and training methodologies must be employed to prevent and detect bias and ensure a high level of performance for all users, regardless of ethnicity, age and gender.

You can read more about biometric inclusivity and accessibility here.

Summary

Following the pandemic, individuals have come to expect that they won't be inconvenienced by in-person appointments to access government services. But this very same convenience of public sector services is making benefits more accessible to fraudsters, too.

This has ushered in an era of colossal public sector fraud wherein criminals are interrupting the flow of humanitarian aid to those in need. It's become an industry for criminal networks, and they are siphoning funds at an alarming rate, empowered by sophisticated and evolving technologies.

Decisive action is needed to stem the crisis that is public sector fraud – identity verification using biometric face verification technology is recommended. This enables governments to be sure that each person applying for public schemes, benefits, or services is genuinely who they claim to be.

Face verification is the most robust method of authenticating user identity online. As Biden articulated, the dollar savings that can be achieved by adopting preventative technology are undeniable.
However, the solution chosen must be inclusive and convenient for all. We have laid out the case for a face biometric solution to lead the fight against the public sector fraud crisis.

iProov technology is already proven at scale with governments across the globe – such as the UK Home Office, The US Department of Homeland Security, Singapore GovTech, and more. You can request a demo of our services today through this link.

contact@iproov.com

iproov.com