U.S. Department of Labor

Office of Inspector General
Washington, DC 20210

MARCH 31, 2023

MEMORANDUM FOR: BRENT PARTON
Acting Assistant Secretary
for Employment and Training

Carolyn R. Hantz

FROM: CAROLYN R. HANTZ
Assistant Inspector General
for Audit

SUBJECT: **Alert Memorandum:** ETA and States Need to Ensure the Use of Identity Verification Service Contractors Results in Equitable Access to UI Benefits and Secure Biometric Data
Report Number: 19-23-005-03-315

The purpose of this memorandum is to alert the Employment and Training Administration (ETA) to urgent equity and security concerns the Office of Inspector General (OIG) has determined need immediate attention while we proceed with our work in this area.

Resulting from the economic impact of the COVID-19 pandemic, unemployment insurance (UI) programs have become a target for fraud with significant numbers of imposter claims being filed with stolen or synthetic[1] identities. Although the exact number of imposter claims is unknown, the OIG previously identified[2] that, from March 28, 2020, through September 30, 2020, 4 states paid $9.9 billion on 1.1 million likely fraudulent claims. Within a state, district, or territory, State Workforce Agencies (SWA) are the organizations responsible for administering their UI programs within federal guidelines, including deterring payments made through willful misrepresentation. To combat imposter claims, 24 of 53 SWAs (45 percent) hired a combined total of 10 identity verification service contractors

[1] A synthetic identity is a false identity created from a combination of real and fake information.
[2] COVID-19: ETA and States Did Not Protect Pandemic-Related UI Funds from Improper Payments, including Fraud or from Payment Delays, Report No. 19-22-006-03-315 (September 30, 2022), https://www.oig.dol.gov/public/reports/oa/2022/19-22-006-03-315.pdf

that used facial recognition technology.[3] The OIG is concerned that the use of identity verification service contractors may not result in equitable and secure access to UI benefits in the processing of UI claims.

Our concerns are based on the following risks. Regarding equity, in 2019, the National Institute of Standards and Technology's (NIST)[4] Information Technology Laboratory reported that it found empirical evidence the algorithms[5] used in current facial recognition technology have a racial and gender bias. Regarding security, our review of agreements between SWAs and identity verification service contractors indicated that up to 15 of 24 (63 percent) states had contracts that did not include the privacy security measures recommended by the National Strategy for Trusted Identities in Cyberspace[6] necessary to protect UI claimants' biometric data,[7] which is a form of personally identifiable information (PII).[8]

These risks must be addressed and mitigated by appropriate oversight and guidance from ETA. While ETA has issued guidance on identity verification and

[3] These data are based on the following survey results. We sent surveys to each of the 46 SWAs that ETA reported as using identity verification service contractors. Ninety-six percent (44 of 46) responded. The District of Columbia's SWA did not respond while the SWA in Kentucky was unable to respond due to a state emergency. Of the 44 respondent SWAs, 24 employed an identity verification services contractor that used facial recognition technology to verify claimants' identity; 7 reported they did not use any identity verification service contractors; and 13 SWAs employed an identity verification contractor that used some other form of identity verification, such as knowledge-based checks.

[4] Founded in 1901, NIST is one of the nation's oldest physical sciences laboratories and a non-regulatory agency. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

[5] An algorithm, according to Cambridge Dictionary, is a set of mathematical instructions or rules that, especially if given to a computer, will help to calculate an answer to a problem.

[6] The National Strategy for Trusted Identities in Cyberspace is a federal government initiative launched in 2011 to encourage private sector actors to adopt measures enhancing privacy of PII on the internet, including biometric data.

[7] NIST defines biometrics as the measurement of physiological characteristics like—but not limited to—fingerprints, iris patterns, or facial features that can be used to identify an individual.

[8] The Department of Labor defines PII as the following: any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address…) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as [PII]. This information can be maintained in paper, electronic, or other media. Guidance on the Protection of Personally Identifiable Information, last accessed November 15, 2022, https://www.dol.gov/general/ppii

also on UI benefit equity, ETA has provided minimal guidance[9] that specifically addresses facial recognition technology in administering UI benefits. Without comprehensive guidance, SWAs are at risk of using technology that discriminates against claimants entitled to receive UI benefits and of not adequately safeguarding claimants' PII.

BACKGROUND: FACIAL RECOGNITION TECHNOLOGY

To assess identity, facial recognition systems perform facial detection, which identifies the location of key facial features such as the eyes and nose. After facial detection, facial recognition systems compare an individual's facial features to one stored photograph or many stored photographs to determine possible matches through one of two different types of matching:

1. **One-to-One Matching** tries to verify identity by confirming that a photograph matches a different photograph of the same person. One-to-one matching is commonly used for authentication purposes, such as unlocking a smartphone or verifying a passport. For example, a facial recognition system may compare uploaded photographs of identity documents—such as a driver's license, state ID, or passport—against an uploaded selfie.[10]

2. **One-to-Many Matching** tries to predict identity by comparing a photograph of a single individual against a gallery of stored photographs of individuals to determine whether there is a potential match. One-to-many matching is often associated with public safety and law enforcement applications where it can be used to aid a search for missing children or help investigators locate suspects.

Facial recognition results depend on how the systems are designed, developed, tested, deployed, and operated. There is no single, standardized system design for facial recognition technologies. Organizations build their systems differently for different environments, and use different terms to describe how their systems work.

[9] The guidance where ETA refers to facial recognition technology can be found in its Unemployment Insurance IT Security Guide, which refers SWAs to NIST Special Publication 800-76-2. That publication contains technical specifications for biometric data for the performance of Personal Identity Verification cards.

[10] A selfie is an image that includes one's self taken using a digital device.

EQUITY: RACIAL AND GENDER BIAS IN FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology is a powerful tool that can assist in preventing fraudulent UI payments. Ninety-two percent (22 of 24) of the respondent SWAs employing contractors that used facial recognition technology reported that using these contractors reduced improper payments, including fraud. While using this technology may assist in reducing improper payments, a series of NIST Information Technology Laboratory reports on the accuracy of facial recognition algorithms[11] identified a demonstrated bias for certain demographic groups.

NIST assesses the accuracy of facial recognition algorithms by measuring the two classes of error the software can make: false positives and false negatives. A false positive means the software wrongly considered photographs of two different individuals to show the same person. A false negative means the software failed to match two photographs that, in fact, show the same person. In the context of UI benefits, a false positive would mean an ineligible claimant would be identified as a legitimate claimant for benefits and a false negative would mean an eligible claimant would be identified as a non-legitimate claimant for benefits.

A December 2019 NIST study[12] identified the following bias-related findings:

- False negative error rates vary strongly by algorithm—from below 0.5 percent to above 10 percent—and are often higher in women and in younger individuals;
- For higher-quality images, false negatives are higher in Asian and American Indian individuals;
- For lower-quality images, false negatives are generally higher in people born in Africa and the Caribbean;
- Consistently across algorithms and datasets, false positives tend to be higher in women than men;
- For one-to-one matching, NIST found higher rates of false positives for Asian and African American faces relative to images of Caucasians;

[11] Corporate research and development laboratories and universities submitted algorithms to NIST. For all the algorithms NIST evaluates, NIST posts performance results on its Face Recognition Vendor Test website, located at: https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0.

[12] Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280 (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf; and NIST website, NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

- Among U.S.-developed algorithms, NIST found similar high rates of false positives in one-to-one matching for Asians, African Americans, and native groups (which include Native American, American Indian, Alaskan Indian and Pacific Islanders); and
- For one-to-many matching, the team saw higher rates of false positives for African American females.

NIST elaborated as follows:

> While it is usually incorrect to make statements across algorithms, we found empirical evidence for the existence of demographic differentials in the majority of the face recognition algorithms we studied…While we do not explore what might cause these differentials, this data will be valuable to policymakers, developers and end users in thinking about the limitations and appropriate use of these algorithms.

Expanding on its 2019 findings, NIST issued a 2022 study[13] that found further evidence of bias:

> Since 2019, it has become apparent that false negative inequities [in face recognition algorithms] are substantially due to poor photography of certain groups including under-exposure of dark-skinned individuals, and that this can be addressed by using algorithms more tolerant of poor image quality or, better, by correcting the capture process with superior cameras, imaging environments[,] and human-factors. At the same time, it is also clear that the much larger false positive variations, which occur even in high-quality photographs, must be mitigated by algorithm developers.

In June 2022, the Government Accountability Office reported[14] findings of racial disparity in benefit receipt in the Pandemic Unemployment Assistance program. For example, in two states, the percentage of Black applicants who received Pandemic Unemployment Assistance was about half that of White applicants, and results from two national surveys show similar disparities in the receipt of UI benefits. According to the Government Accountability Office, various factors could explain these disparities, such as how states reviewed claims or whether fraudsters more frequently used certain demographics when filing.

[13] Face Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials. NISTIR 8429 (July 2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8429.ipd.pdf

[14] Government Accountability Office, Pandemic Unemployment Assistance: Federal Program Supported Contingent Workers Amid Historic Demand, but DOL Should Examine Racial Disparities in Benefit Receipt, GAO-22-104438 (June 7, 2022), https://www.gao.gov/products/gao-22-104438

ETA and SWAs must exercise extreme caution to ensure claimants are not subjected to discrimination by the use of facial recognition technology when applying for UI benefits. SWAs that use facial recognition identity verification service contractors typically route the UI benefit claimant to the contractors' website for identity verification. A claimant is then asked to provide a facial photograph. Claimants who cannot complete the identity verification process are provided a range of alternatives by the various SWAs. Specifically, claimants are provided the following options or combination of options: claimants must apply with paper, mail, fax, telephone, or email; claimants must visit a local American Job Center or SWA office; a SWA or contractor performs additional verification; or the claimant is denied benefits and must start an adjudication process.

However, even with the alternatives, prior studies have shown that claimants of certain races and genders will likely have better access to UI benefits. Additionally, facial recognition technology is largely dependent on the photograph the claimant submits. Claimants that do not have advanced technological skills or use outdated technology are less likely to be able to submit a high-quality photograph and pass facial recognition eligibility procedures.

In July 2022, ETA issued Unemployment Insurance Program Letter No. 17-22, which reminded states that a top priority of the U.S. Department of Labor is ensuring equitable and meaningful access to the UI program. The program letter also stated that the U.S. Department of Labor interprets Section 303(a)(1) of the Social Security Act to include a requirement of UI benefit equity. Additionally, the program letter stated the following:

> [S]tate UI agencies must ensure use of technologies and systems for administering UI programs and providing services do not create barriers (e.g., procedural, technological, or informational) that may prevent individuals from accessing [unemployment compensation] benefits, such as by denying them a reasonable opportunity to establish their eligibility.

Additionally, ETA encouraged states to examine any available claimant demographic data to help inform strategies to enhance outreach and education about underserved communities. Further, ETA encouraged states to explore strategies to improve their state's UI program recipiency rate.

When we inquired with ETA about steps states had taken to identify bias in facial recognition technology, ETA recognized the challenge that some states identified associated with the technology but was unaware of specific efforts taken by states to test for bias within their programs.

The OIG notes that the Oregon Employment Department acted following media-expressed concerns regarding identity verification service contractors and their use of facial recognition software. The Oregon Employment Department had contracted with an identity verification service contractor for all regular UI and Pandemic Unemployment Assistance claims. The automated processes required claimants to verify their identity before UI benefits were paid. The Oregon Employment Department paused the automated process to perform an internal study to determine whether there were disparate impacts among various demographic groups.

The study measured claimants within multiple demographic groups to review the rate at which the people referred to the identity verification service contractor completed the identity verification process. The study identified differences in completion rates among some demographic categories; however, it did not show causation for these impacts. As a result of the study, the Oregon Employment Department conducted a claimant outreach campaign and based on the campaign designed mitigation strategies. Additionally, the Oregon Employment Department shared the results of the study with other states.

ETA recently initiated a Claimant Experience Pilot Project to test an improved process for completing initial intake questions and identity proofing while keeping equity, fraud prevention, and claim timeliness at the forefront. Through this effort, the Arkansas Division of Workforce Services is piloting the General Services Administration’s Login.gov. This is a shared sign-on service that has expanded since its inception to offer identity proofing capabilities as a digital alternative to the state’s in-person identity verification process. ETA is evaluating whether this may be a possible solution for use in the UI program. In March 2023, this pilot was expanded to include an in-person identify proofing pilot with the U.S. Postal Service. DOL anticipates expanding the pilots to additional states. However, in lieu of an ETA-approved and universally adopted identity verification method, ETA must provide guidance to states on the current facial recognition technologies in use.

SECURITY AND IDENTITY VERIFICATION SERVICE CONTRACTORS

Contractors that use facial recognition technology have access to a large amount of highly-sensitive PII. The risks associated with a biometric data breach raises serious privacy concerns for both the public and the government. Compared to a username or password, which could be changed after a breach, biometric data is at greater risk from a data breach. The nature of biometric data means that it cannot be changed.

Further, SWAs using identity verification service contractors that use facial recognition technology are compelling claimants to submit biometric data to receive unemployment compensation that they are entitled to by state and federal law. Without contract protections in place, the biometric data is at-risk of being used for other purposes.

There is no comprehensive federal privacy law governing the collection, use, and sale or other disclosure of personal data by private-sector companies. In the absence of federal law or national guidance, some states have taken varied approaches to facial recognition technology, including:

- Colorado requires that, prior to the state procuring or internally developing identity verification services, the state will publish an extensive accountability report on the facial recognition service and will update that report at least every 2 years;
- Maine prohibits the use of facial recognition technology for any identity verification with a few exceptions such as for the investigation of a serious crime; and
- Vermont enacted a near-total moratorium on facial recognition, prohibiting its use in almost all situations except for investigations related to sexual exploitation of minors and as permitted with respect to drones.

Therefore, it is up to ETA and SWAs that authorize the use of facial recognition technology to provide consistent guidance and adequate oversight to ensure data related to UI claims is adequately protected.

While there is no comprehensive federal privacy law, in April 2011, the federal government announced the National Strategy for Trusted Identities in Cyberspace to improve the privacy, security, and convenience of sensitive online transactions through collaborative efforts with the private sector, advocacy groups, government agencies, and other organizations. The strategy specifically calls for improved privacy protection for individuals and advises[15] the following privacy protection measures:

- Limit the collection and transmission of information to the minimum necessary to fulfill the transaction's purpose and related legal requirements;
- Limit the use of the individual's collected and transmitted data to specified purposes;
- Limit the retention of data to the time necessary for providing and administering the services to the individual end-user for which the data was collected, except as otherwise required by law;
- Provide concise, meaningful, timely, and easy-to-understand notice to end-users on how providers collect, use, disseminate, and maintain personal information;
- Establish accuracy standards for data used in identity assurance solutions;

[15] NIST, Standards for Biometric Technologies, https://www.nist.gov/speech-testimony/standards-biometric-technologies

- Protect, transfer at the individual's request, and securely destroy information when terminating business operations or overall participation in the Identity Ecosystem;[16] and
- Be accountable for how information is actually used and provide mechanisms for compliance, audit, and verification.

To assess the services provided by identity verification service contractors on behalf of the 24 SWAs, we reviewed contract terms and agreements. We identified 5 primary issues with the contracts between the SWAs and 10 different identity verification service contractors (see Table 1).

Table 1: States with Missing Contract Elements that May Affect Security

Missing Element(s)	No. of States with Missing Contract Elements	No. of States that use Facial Recognition Technology	% of Total
No clear identification whether the contractor would use one-to-one or one-to-many matching*	18	24	75%
Did not address the requirements for data storage**	15	24	63%
Did not address the requirement for destroying or disposing of data collected**	13	24	54%
No indication of the identity standards for facial recognition**	10	24	42%
No indication of the method for compliance, audit, or verification**	6	24	25%

* The use of one-to-one and one-to-many matching are not recommended National Strategy for Trusted Identities in Cyberspace privacy protection measures. However, NIST identified separate bias issues associated with the different types of matching. Therefore, states should ensure the matching type is clearly identified in contracts.
** These contract elements were based upon the privacy security measures recommended by the National Strategy for Trusted Identities in Cyberspace.
Source: OIG review of identity verification service contracts

[16] The National Strategy for Trusted Identities in Cyberspace is focused on the creation of an "Identity Ecosystem" where all Americans can choose from a variety of identity solutions that enable more secure, convenient and privacy-enhancing experiences everyplace they go online. Biometrics are one of many types of identity solutions that will play a role in the Identity Ecosystem.

Identity verification service contractors may have implemented data storage, destruction, facial recognition standards, or compliance protections on their own or SWAs may not have provided all the contract elements. However, without ETA providing guidance on all the advised protections for biometric information, including those collected during facial recognition, SWAs may not include sufficient contract requirements to adequately protect claimants' PII or to protect claimants from discriminatory misidentification.

Recommendations

We recommend the Acting Assistant Secretary of Employment and Training:

1. Provide guidance that ensures SWAs provide upfront, clear, consistent, and fair alternatives to services that rely on facial recognition technology.

2. Require SWAs that use facial recognition technology to test the system for biases and design procedures to mitigate those effects. SWAs need to report findings from bias testing to ETA regarding implementation or use of identity verification services that rely on facial recognition technology.

3. Provide guidance to SWAs to help ensure that contracts with identity verification service providers include requirements on the secure storage of data, destruction of the data once the contract is concluded, and purging of any large datasets collected by identity verification service providers on a regular basis.

Summary of ETA's Response

On March 29, 2023, ETA provided us their formal response to the draft alert memorandum and recommendations (see Attachment). ETA expressed its appreciation for the OIG's work and welcomed the OIG's input. Further, ETA agreed with our three recommendations and, by September 30, 2023, will issue guidance addressing each recommendation.

The OIG appreciates the response and the efforts ETA is making to improve equitable access to UI benefits and to secure claimants' biometric data. For example, ETA included reminders in its guidance that program integrity efforts must also ensure eligible individuals have equitable access. However, when we reviewed the information provided by ETA on December 29, 2022, we did not find specific examples of steps states have taken to identify and mitigate bias in facial recognition technology. We look forward to working with ETA to address this area of concern. The OIG also appreciates ETA's commitment to implementing the OIG's recommendations by specifically addressing challenges with facial recognition technology in UI programs.

Attachment

U.S. Department of Labor

Employment and Training Administration
200 Constitution Avenue, N.W.
Washington, D.C. 20210

March 29, 2023

MEMORANDUM FOR: CAROLYN R. HANTZ
Assistant Inspector General for Audit

FROM: BRENT PARTON
Acting Assistant Secretary

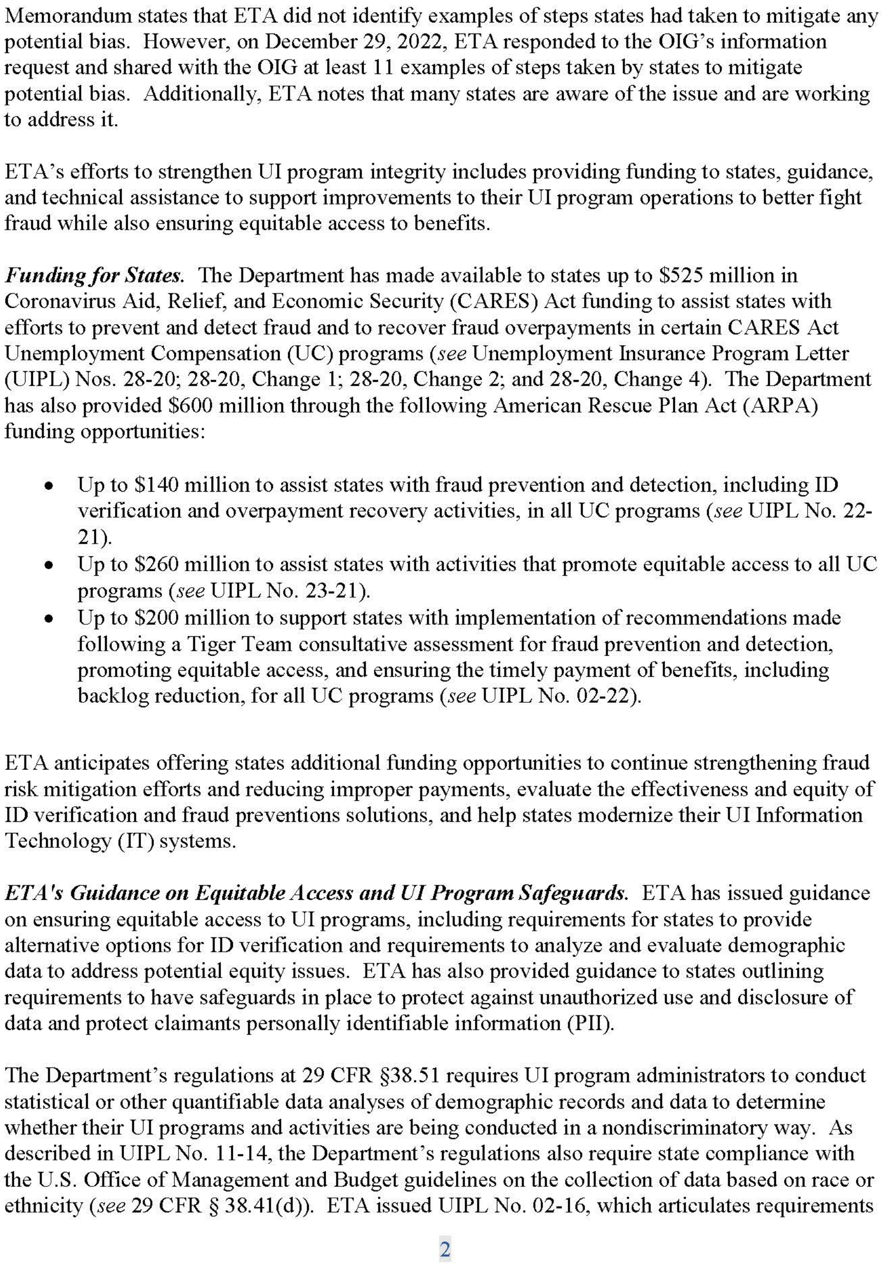
SUBJECT: Response to Draft Alert Memorandum: *ETA and States Need to Ensure that Identity Verification Contractors Provide Equitable Access to Unemployment Insurance Benefits and Secure Storage and Destruction of Biometric Data,* Report Number: 19-23-00X-03-315

The Department of Labor's (Department) Employment and Training Administration (ETA) appreciates this opportunity to respond to the above-referenced Office of Inspector General (OIG) draft alert memorandum.

ETA appreciates your study of states' use of facial recognition technology as part of their identity (ID) verification efforts. ID verification is an area that ETA believes the federal government can play a larger role in supporting the Unemployment Insurance (UI) system and helping states in the administration of the UI program. As noted in the Alert Memorandum, the Department is currently pursuing pilot projects to explore a possible national solution to be made available for use by states. As with any integrity and fraud prevention efforts, ETA must promote solutions that does not have unintended negative impacts on equitable access to UI benefits. Again, ETA welcomes the OIG's input on this topic as it remains committed to ensuring UI program integrity and equitable access to benefits continue to be top agency priorities.

States faced significant challenges combatting the substantial increase in sophisticated ID fraud that targeted state UI programs across the nation during the pandemic. In response, many states rapidly contracted with service providers to implement new technologies and services aimed at preventing and detecting fraud, including solutions to strengthen state ID verification processes. Prior to the pandemic, these were often manual processes. ETA recognized that many of these ID verification service provider solutions used biometric data, and some used facial recognition technology. While states have been aggressively addressing fraud and implementing these solutions for the UI programs, ETA included reminders in its guidance that program integrity efforts aimed at preventing fraudulent activity must also ensure eligible individuals with legitimate claims have equitable access to receive the benefits they are entitled to when they are due.

ETA notes that one statement in the Alert Memorandum does not fully convey actions already taken by states to address potential bias using facial recognition technology. The Alert



Memorandum states that ETA did not identify examples of steps states had taken to mitigate any potential bias. However, on December 29, 2022, ETA responded to the OIG's information request and shared with the OIG at least 11 examples of steps taken by states to mitigate potential bias. Additionally, ETA notes that many states are aware of the issue and are working to address it.

ETA's efforts to strengthen UI program integrity includes providing funding to states, guidance, and technical assistance to support improvements to their UI program operations to better fight fraud while also ensuring equitable access to benefits.

Funding for States. The Department has made available to states up to $525 million in Coronavirus Aid, Relief, and Economic Security (CARES) Act funding to assist states with efforts to prevent and detect fraud and to recover fraud overpayments in certain CARES Act Unemployment Compensation (UC) programs (*see* Unemployment Insurance Program Letter (UIPL) Nos. 28-20; 28-20, Change 1; 28-20, Change 2; and 28-20, Change 4). The Department has also provided $600 million through the following American Rescue Plan Act (ARPA) funding opportunities:

- Up to $140 million to assist states with fraud prevention and detection, including ID verification and overpayment recovery activities, in all UC programs (*see* UIPL No. 22-21).
- Up to $260 million to assist states with activities that promote equitable access to all UC programs (*see* UIPL No. 23-21).
- Up to $200 million to support states with implementation of recommendations made following a Tiger Team consultative assessment for fraud prevention and detection, promoting equitable access, and ensuring the timely payment of benefits, including backlog reduction, for all UC programs (*see* UIPL No. 02-22).

ETA anticipates offering states additional funding opportunities to continue strengthening fraud risk mitigation efforts and reducing improper payments, evaluate the effectiveness and equity of ID verification and fraud preventions solutions, and help states modernize their UI Information Technology (IT) systems.

ETA's Guidance on Equitable Access and UI Program Safeguards. ETA has issued guidance on ensuring equitable access to UI programs, including requirements for states to provide alternative options for ID verification and requirements to analyze and evaluate demographic data to address potential equity issues. ETA has also provided guidance to states outlining requirements to have safeguards in place to protect against unauthorized use and disclosure of data and protect claimants personally identifiable information (PII).

The Department's regulations at 29 CFR §38.51 requires UI program administrators to conduct statistical or other quantifiable data analyses of demographic records and data to determine whether their UI programs and activities are being conducted in a nondiscriminatory way. As described in UIPL No. 11-14, the Department's regulations also require state compliance with the U.S. Office of Management and Budget guidelines on the collection of data based on race or ethnicity (*see* 29 CFR § 38.41(d)). ETA issued UIPL No. 02-16, which articulates requirements under federal law to ensure access to UI benefits and provides guidance to assist states to meet those requirements. This guidance requires state UI agencies to ensure that use of new technologies and systems for administering UI programs and providing services do not create barriers (*e.g.*, procedural, technological, or informational) that may prevent individuals from accessing UI benefits, such as by denying them a reasonable opportunity to establish their eligibility. UIPL No. 02-16, Change 1, highlights additional state responsibilities regarding access to UI benefits. Furthermore, UIPL No. 16-21, discussed how states may use a variety of mechanisms to verify an individual's ID (*e.g.*, submit documents on-line, report in-person, or complete a questionnaire) and required states to provide alternative mechanisms for individuals with access barriers. The fundamental importance of equitable access is further emphasized as one of the three pillars under Section 9032 of ARPA[1] and as a national priority in the Fiscal Year 2023 State Quality Service Plan Additional Planning Guidance (*see* UIPL No. 17-22).

Regulations related to confidentiality and disclosure of state UC information are published at 20 CFR Part 603. States may disclose confidential UC data when necessary for the proper administration of the UC program. ETA has also provided guidance to states regarding the use of data contract protections. This guidance was addressed in Section 5 of UIPL No. 12-01, Change 2, where states were advised that contractors acting directly on behalf of the state agency are subject to the same requirements as state employees to maintain the confidentiality of the UC data. States must ensure a written, enforceable, and terminable agreement with contractors, that provides basic safeguards, including a provision for safeguarding information against unauthorized access or redisclosure as described in 20 C.F.R. 603.9. ETA provided states with an updated version of the UI IT security guide and highlighted information on IT security guidance from the National Institute of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS), including standards on protecting PII in state UI IT systems and biometric specifications for person ID verification (*see* UIPL No. 04-21).

Investments in UI Program Integrity. ETA continues to invest in developing new and enhancing existing tools, datasets, and resources and making these available to states to aid states with quickly identifying potential fraud and improving ID verification in UC programs. In the Alert Memorandum, the OIG acknowledges the Department's ongoing pilot work with the General Services Administration's Login.gov to provide an online ID verification option and its recent work with the U.S. Postal Service to provide an in-person ID verification for UI services. The Department plans to expand the availability of these service to other states.

Response to the OIG Recommendations

ETA is committed to continuing its work with states to ensure equitable access to UI programs and will implement the OIG's recommendations by specifically addressing challenges with facial recognition technology in UI programs. Below, please find each of the OIG's recommendations contained in this Alert Memorandum followed by ETA's response and proposed action steps to address them.

[1] Section 9032 of ARPA provides a $2.0 billion appropriation to the Secretary of Labor to: (1) detect and prevent fraud; (2) promote equitable access; and (3) ensure the timely payment of benefits with respect to unemployment compensation (UC) programs.

Attachment

<u>Recommendation 1</u>: Provide guidance that ensures [State Workforce Agencies (SWAs)] provide upfront, clear, consistent, and fair alternatives to services that rely on facial recognition technology.

<u>ETA Response</u>: ETA concurs with this recommendation and will issue additional guidance requiring states to provide at least one timely, effective, and accessible non-digital alternative to online ID verification. ETA will emphasize that the non-digital option should not be overly burdensome to applicants, and limit access to public benefits programs or the timely receipt of benefits to eligible individuals. The Administrator for the Office of Unemployment Insurance is responsible for the implementation of this recommendation. ETA anticipates completion of the correction actions by September 30, 2023.

<u>Recommendation 2</u>: Require SWAs that use facial recognition technology to test the system for biases and design procedures to mitigate those effects. SWAs need to report findings from bias testing to ETA regarding implementation or use of identity verification services that rely on facial recognition technology.

<u>ETA Response</u>: ETA concurs with this recommendation. As mentioned above, the Department's regulations and guidance already require state UI programs to collect and analyze claimant demographic data for possible indications of systemic discrimination and investigate any such indications of potential discrimination that the analyses provide.

ETA will issue additional guidance highlighting that states should work with their service providers to identify and resolve any barriers or equitable access impacts resulting from ID proofing practices. ETA will explore options to have states that use facial recognition technology in their ID verification process provide information on the results of their evaluations and the actions they took to mitigate equity issues. The Administrator for the Office of Unemployment Insurance is responsible for the implementation of this recommendation. ETA anticipates completion of the correction actions by September 30, 2023.

<u>Recommendation 3</u>: Provide guidance to SWAs to help ensure that contracts with identity verification service providers include requirements on the secure storage of data, destruction of the data once the contract is concluded, and purging of any large datasets collected by identity verification service providers on a regular basis.

<u>ETA Response</u>: ETA concurs with this recommendation. As outlined above, rules regarding confidentiality and disclosure of state UC information are outlined in federal regulation (*see* 20 CFR Part 603). Also, ETA has provided guidance to states regarding contractors and safeguarding information against unauthorized access or redisclosure and protecting PII. ETA will issue additional guidance to states that includes recommended contract provisions states should consider concerning service providers delivering ID proofing solutions and services. The Administrator for the Office of Unemployment Insurance is responsible for the implementation of this recommendation. ETA anticipates completion of the correction actions by September 30, 2023.