EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U.S. DEPARTMENT OF LABOR Washington, D.C. 20210	CLASSIFICATION Unemployment Insurance
	CORRESPONDENCE SYMBOL OUI/DUIO
	DATE April 13, 2021

ADVISORY: UNEMPLOYMENT INSURANCE PROGRAM LETTER NO. 16-21

TO: STATE WORKFORCE AGENCIES

FROM: SUZAN G. LEVINE
Principal Deputy Assistant Secretary

SUBJECT: Identity Verification for Unemployment Insurance (UI) Claims

1. **Purpose.** To highlight the importance of identity verification in ensuring the proper payment of unemployment benefits and to provide guidance to states on required administrative procedures when processing claims and determining UI eligibility in cases where an individual's identity (ID) is questionable.

2. **Action Requested.** The U.S. Department of Labor's (Department) Employment and Training Administration (ETA) requests that State Administrators provide this information to appropriate staff.

3. **Summary and Background.**

   a. Summary – UI integrity is a top priority of the Department and State Workforce Agencies. The Department supports states' efforts to verify ID as part of the UI claims process in order to stop fraudulent claims using stolen personally identifiable information (PII), including Social Security Numbers (SSN). In resolving issues related to ID verification, states must follow the adjudication standards outlined in sections 303(a)(1) and 303(a)(3) of the Social Security Act (SSA) (42 U.S.C. 503(a)(1) and (3)) and the Standard for Claim Determination (CD) (20 C.F.R. Part 614, Appendix B). When ID issues arise through a crossmatch with a federal database, the Computer Matching and Privacy Protection Act of 1988 (CMPPA), 5 U.S.C. 552a(o)-(r), also applies.

   As states consider new and evolving ID verification tools and strategies, the Department has become aware of some uncertainty among states about the administrative processes that are required when resolving issues of questionable ID.

   This UIPL provides guidance to states about the adjudication standards as they apply specifically when processing claims and determining UI eligibility in cases where an individual's ID is questionable.

RESCISSIONS None	EXPIRATION DATE Continuing

In addition to the content described in this UIPL, for resources, recommendations, and best practices regarding identity verification and combatting identity theft and fraud, including data analytics, prevention, detection, and recovery activities, please visit the UI Integrity Center's Knowledge Exchange Library. ETA strongly encourages state workforce agencies to align their state website content and communications for victims of unemployment identity theft with the content, resources, and reporting requirements outlined at www.dol.gov/fraud.

b. Background – Section 303(a)(1) of the SSA, requires that a state have methods of administration to reasonably ensure the full payment of unemployment compensation when due. In addition, Section 1137(a)(1), SSA, requires states to require the individual to furnish their Social Security Number as a condition of eligibility for benefits. These Federal provisions mean, among other things, that a state must have a system to reasonably ensure that the name and Social Security Number used to establish eligibility for unemployment compensation belong to the individual filing the claim. UIPL No. 35-95 also outlines that the provision of an individual's SSN is a requirement for claimstaking.

Since the unprecedented increase in claims resulting from the economic impact of the Coronavirus Disease 2019 (COVID-19) pandemic, UI programs have become a target for fraud with significant numbers of imposter claims being filed with stolen or synthetic identities. Synthetic identity fraud occurs when real and fake information are combined to create false identities. Additionally, fraudulent employers report fabricated wages for real individuals or use synthetic identities to have the fabricated wages appear to have been earned in the base period and then those associated employees file fraudulent UI claims based on these fabricated wages. Because synthetic identities combine multiple data points, it is more difficult to prevent and detect this type of fraud, requiring the use of crossmatches with additional data sources to support detection.

The Unemployment Insurance Fraud Protection Guide issued by the U.S. Department of Justice on September 21, 2020, page 1, states: "Fraudsters, some of which are transnational criminal organizations, are using stolen identities of U.S. citizens to open accounts and file fraudulent claims for UI Benefits, exploiting the unprecedented expansion of these benefits provided in response to economic disruption caused by the COVID-19 pandemic." (See https://www.justice.gov/file/1324726/download)

ID theft is not only a major concern for the UI programs but also a growing nationwide and worldwide problem. Recognizing this dilemma, Congress passed Public Law 105-318, which modified 18 U.S.C. § 1028 ("Fraud and related activity in connection with identification documents, authentication features, and information") to make it a federal crime for whoever "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law." 18 U.S.C. 1028(a)(7). In 2019, the Federal Trade Commission received over 650,000 reports of ID theft and in recent years, state UI systems have identified multiple fraud schemes involving stolen Personally Identifiable

Information (PII). According to the Identity Theft Resource Center, government ID theft occurs when a victim's sensitive PII is used to obtain funds and/or services from federal or state governments (https://helpcenter.idtheftcenter.org/s/).

States are employing a wide array of strategies to verify the identities of UI claimants through crossmatches, state developed tools, and private vendor services. In addition, the UI Integrity Center's Integrity Data Hub (IDH) is making new data sources available for states' use, such as its Identity Verification (IDV) solution.

The IDH provides states a secure and centralized system, containing various datasets, to assist states in detecting and preventing fraud, identity theft, and improper payments in the unemployment insurance program. In essence, states send their unemployment insurance claims data to the IDH, which the IDH crossmatches against a variety of datasets to determine if a claim has suspicious attributes that may indicate fraud or identity theft.

4. Claims Determination Processes Related to ID Verification.

When a state obtains information through automated systems or other sources that question whether the name and/or SSN used to file a claim belong to the individual who is filing the claim, the state must act quickly to: i) provide the individual with proper notice and an opportunity to provide information to resolve the issue; ii) decide whether or not sufficient information has been provided to verify the individual's ID; and iii) issue a written determination. The notice must also include information that failure to respond could result in a determination denying benefits and establishing an overpayment of any benefits previously paid. These processes must be consistent with the adjudication standards of sections 303(a)(1) and 303(a)(3) of the SSA (42 U.S.C. 503(a)(1) and (3)), and the CD (20 C.F.R. Part 614, Appendix B).

If the information that creates the ID issue is obtained from a federal database, the state must follow the requirements of the CMPPA. Section 4.g. of UIPL No. 01-16 discusses these requirements in detail. The CMPPA does not apply when states are using their own internal data or non-federal databases, such as the UI Integrity Center's IDH, though states must still conform to the adjudication standards described in this UIPL when resolving the question of an individual's ID raised by a non-federal database. ETA funds the UI Integrity Center through a cooperative agreement with the Center for Employment Security Education and Research (CESER) (a subsidiary of the National Association of State Workforce Agencies (NASWA), which is an organization representing state workforce agencies). The UI Integrity Center operates the IDH. ETA does not store or have access to any IDH data.

States must act promptly to verify an individual's ID in order to meet the requirement of section 301(a)(1), SSA, that the state have methods of administration reasonably calculated to ensure full payment of UI when due. For new claims, payment "when due" means that qualified and eligible individuals receive their first benefit payments as soon as administratively feasible. Refer to subsection b, Adjudication of ID Verification Issues, below regarding the "when due" requirement applicable to continued claims.

UIPL No. 04-01 interprets the "when due" requirement to also require states to ensure that payment of benefits is not made when payment is not due. Investigations of fraudulent imposter claims involving claimants, employers, and/or state staff are necessary for the proper administration of the UI program. States must have processes in place to ensure benefits are only paid to the individual whose identity has been verified. However, once a claim has been established and payments have been issued, there is a presumption of eligibility (refer to UIPL 04-01). Therefore, there must be evidence on the record that substantiates a reasonable basis for stopping payments once a determination of eligibility has been made and payments have been issued.

a. **ID Verification Processes**

Acceptable documents to verify ID are documents made or issued by or under the authority of the United States Government, any of the states (including the District of Columbia, the Commonwealth of Puerto Rico and the U.S. Virgin Islands), political subdivisions of a state, a foreign government, a political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals. Some examples of acceptable identification documents include, but are not limited to, Social Security cards, birth certificates, driver's licenses, government passports, alien registration cards, and other government issued identification cards. Limiting the acceptable documents that may be used for ID verification in this manner is consistent with 18 U.S.C. 1028(d)(3), which addresses fraud and related activity in connection with identification documents. Because these types of documents are the most reliable for verifying identity and preventing fraud, this requirement is a reasonable interpretation of the SSA section 303(a)(1) obligation to provide "[s]uch methods of administration … as are found by the Secretary of Labor to be reasonably calculated to insure full payment of unemployment compensation when due."

A state's list of acceptable documents to verify ID must include a sufficient variety to provide for equal access to UI benefits for all claimants. For example, if the state requires a state driver's license as proof for ID verification, it must offer a reasonable alternative for those who may not have that type of identification or provide sufficient time for other means of identification to be obtained.

Suspicious claims may be flagged at three different times during the claims filing process. We provide scenarios describing the timing of each, the issue to be resolved, and instructions for how the state reports such activities. When a suspicious claim is flagged for ID verification in all three of these scenarios, the state's request for additional information and resolution of the issue must align with the notice requirements discussed in subsection c, Requirements for Processes to Verify Identity, below.

Timing of ID verification issues.

As mentioned above, there are three times in the life cycle of a claim when ID verification may occur:

1. After an application is received by the state, but before the application is entered into the state's benefit system (e.g., the state presents ID verification questions and only allows the claim to be processed when the applicant is able to correctly answer the ID verification questions);
2. After a claim is filed, but before payment is issued (e.g., the state identifies potential ID verification issues during the claim filing process, but accepts the claim and requests the claimant provide proof of ID before payments are made); and
3. After a claim is filed and payments have been issued.
    a. The state became aware of the ID issue through its normal processes of issue identification (e.g., the state receives information that the individual who filed the claim is not the owner of the wages or the identity used on the claim or the claim is "hijacked" by an imposter after the owner of the wages/identity files a legitimate claim).
    b. A financial institution identifies suspicious activity and contacts the state to return funds (refer to subsection b below).

Possible outcomes of an attempt to verify ID.

If the claimant provides the requested information and the state is able to verify the claimant is the owner of the wages used to file the claim, the issue is resolved and the claimant is eligible for benefits, as long as the claimant otherwise meets all other eligibility requirements.

If the claimant does not respond to the request for information and the state is unable to verify the claimant's ID, the state must issue an immediate prospective denial based on a failure to respond (see subsection c, Requirements for Processes to Verify Identity, below for additional instructions). The issuance of a prospective denial for failure to respond does not preclude the state from continuing to investigate potential fraud for any weeks that have already been paid. If the claimant does not respond to the request to provide proof of identity and the state is unable to verify the claimant's identity, and no payments have been made on the claim, the state may disqualify the claimant for failure to respond to a request for information from the beginning of the claim. Such denial may continue indefinitely until the individual reports or provides information as directed.

If the state conducts an investigation and determines that the individual who filed the claim (or in the case of a claim that was "hijacked," the individual who was paid the benefits) is not the owner of the wages/identity, the state must issue a determination based on the identity not being verified, issue a fraud determination, and establish a fraud overpayment (see subsection c, Requirements for Processes to Verify Identity, below for additional instructions).

b. **Adjudication of ID Verification Issues**

States must determine a claimant's eligibility whenever an ID verification issue arises. The adjudication process must conform to the adjudication standards detailed in this UIPL, including: i) providing the individual with proper notice and an opportunity to provide information to resolve the issue; ii) deciding whether or not sufficient information has been provided to verify ID; and iii) issuing a written determination.

ETA strongly recommends that states redact the employer information (i.e., name of employer and Employer ID information) on the monetary determinations when ID theft is suspected during the initial claim process.

For ID verification issues that arise after the initial claim is filed and benefit payments have been issued, the state must determine if it is appropriate to pause payment while the identity verification is being conducted. To do so, the state must have evidence on the record that substantiates a reasonable basis for establishing the issue and pausing payment (*e.g.*, the state has identified potential fraud based on its own data analytics).

If the state determines that it is appropriate to pause payment while the identity verification is being conducted, the state is not required to issue payment for the week in question until it issues a determination of eligibility or ineligibility, as long as the determination is timely. For continued claims, timely payment (i.e., payment "when due") means that a determination is made no later than the end of the week following the week in which the issue is detected. If the decision is not issued timely, the state must continue to pay the continued claim and issue a determination as soon as administratively feasible after payment is made. (See UIPL No. 01-16 and UIPL No. 04-01.)

A financial institution's decision to return UI benefit payments to the state is not sufficient, on its own, to determine benefits have been overpaid or that fraudulent activity occurred. If the state has not already done so, the state must verify the individual's identity.

If the financial institution does not provide any details on why the payments were returned and the state has no other information to indicate suspicious activity occurred, the state may not stop payments to the individual while conducting the ID verification process. The state must have a process to reissue any benefits as soon as administratively feasible and through an alternative method (e.g., new direct deposit account, debit card, paper check). This process must include contacting the claimant to update the payment method. (See UIPL No. 02-16, Section 4A)

Timely determinations prevent fraudulent benefit payments while ensuring that qualified and eligible claimants receive benefits as soon as administratively feasible.

c. **Requirements for Processes to Verify Identity**

The CD standards set forth at 20 C.F.R. Part 614, Appendix B, apply to all eligibility issues identified throughout the continued claim cycle, including ID verification issues. These requirements, as they apply specifically to ID verification, are discussed in detail below.

- Proper Notice. The state's first step after a question of ID arises is to notify the individual of the issue and that ID verification is required. The notice must provide clear instructions for the individual to meet the requirement by providing: 1) an explanation of the issue; 2) the types of documentation accepted by the agency as proof to verify ID; 3) instructions on where/how/to whom the information must be provided; and 4) the consequences of not responding timely, including that the consequences for failure to respond could result in a determination denying benefits and establishing an overpayment of any benefits previously paid. The notice must also include a reasonable deadline by which the individual is to provide the requested information.

  The state must use the contact information provided by the individual filing the claim. (See sections 6012 A, 6013 A.1, and 6015 of the CD.) In addition, and separate from the notification, if the state posts such notice(s) on a claimant portal, the message must remain in the claimant's login portal until the issue has been resolved.

  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). States must provide alternative mechanisms for individuals with access barriers, such as a disability or limited English proficiency. (See Sections 5-9 of UIPL No. 02-16)

- Written Determination. If the individual does not respond timely or responds but does not provide adequate information, the state must provide a written determination in accordance with section 6013 C.1.c. of the CD ("[t]he agency must give each claimant a written notice of … [a]ny…determination which adversely affects a claimant's right to benefits"). The determination must explain the reason for the decision, including the facts: what the individual was asked to provide; what was received; and, if information was received, why that information was insufficient to verify the individual's ID.

  In accordance with section 6012 C of the CD, the state must keep a record of the facts used in its determination.

  Notice of appeal rights. The written determination must give the claimant the option to appeal the determination or to ask for reconsideration, as required by sections 6012 A, 6013 C.2., and 6013 C.2.i. of the CD.

While an individual's failure to respond is sufficient to prevent additional benefits from being paid until the individual responds, failure to respond in and of itself is not sufficient to establish an overpayment. The state must consider the evidence supporting suspicious activity, in addition to the individual's failure to respond to the state's attempt to verify identity, and determine if, under state law, the evidence in the record is sufficient to establish an overpayment. Application of state law informs whether the overpayment is considered fraudulent or non-fraudulent based on the facts and evidence in the claim file.

The agency must keep a written record of the facts considered in reaching its determination. Examples of evidence supporting suspicious activity may include, but are not limited to:

- IDH matches indicating suspicious claims data;
- IDV score below the state's established threshold;
- Crossmatches with Federal, state and/or local databases indicating suspicious activity;
- Crossmatches with private-sector databases indicating suspicious activity;
- Data analytics from state developed tools or private vendor services detect suspicious activity such as:
    - Multiple claims using the same Internet Protocol (IP) address, mailing address, email address, phone number, bank account, security answers, or other data elements;[1]
    - Multiple claims with trends in days or times that claims are filed;
    - SSN used on claims in multiple states;
    - Physical or mailing address belongs to a vacant property or fictitious address;
    - Out-of-country IP address;
    - Phone number with an invalid area code;
    - Email address using a domain frequently identified as fraudulent;
    - Mismatched city and county information;
    - Time spent filing the claim is significantly quicker than the median filing time.
- Employer or Employer Representative indicates no record of employment or reports the individual never worked for them;
- Claim tied to fictitious employer investigation or determination;
- Benefit payment rejected by a bank or financial institution;
- Claimant requests to change the bank account for direct deposit;
- A statement from the alleged victim of ID theft.[2]

[1] It is important to recognize that there are legitimate instances of multiple claimants using the same IP addresses when accessing the state UI system, such as individuals using computers at local libraries, legal aid office, or at America Job Centers. Similarly, there are legitimate instances of multiple claimants using the same mailing address, such as residents of Domestic Violence Safe Houses, homeless shelters, or other communal living locations. State UI agencies are encouraged to identify these types of legitimate multiple user indicators and ensure they do not get included as indicators of suspected fraudulent activities.

Fraud determinations may not be made by an automated system. The written determination must be sent to the individual who filed the claim (i.e., the imposter), using the address provided when the claim was filed (see UIPL 01-16).

Denial for failure to respond. If a claimant is required to verify their ID and fails to respond to the request, provided state law allows, the state may deny benefits as of the date the individual failed to report or respond to the request for information. Such denial may continue indefinitely until the individual reports or provides information as directed. However, if the facilities or systems to which the individual was directed to report are unavailable (e.g., unable to report in-person because the office is closed), no denial can be issued for that week.

States must send a written determination to individuals who are denied for failure to respond. When the individual is denied for failure to respond as requested to verify their ID, to mitigate unnecessary appeal hearings, we strongly recommend that states include instructions in the written determination explaining how they can comply with the reporting requirements.

d. **Reporting**

Determinations related to ID verification may affect the claimant's monetary determination. The state must report this only in two places: 1) the original monetary determination on the ETA 218 – Benefit Rights and Experience report; and 2) the nonmonetary redetermination in column 17 – "Other (Aliens, Athlete, School)" of the ETA 207. A monetary redetermination issued as a result of the nonmonetary determination is not reportable.

Currently, there is no mechanism for states to report ID verification issues when the ID verification determination results in the denial of the claim before the claim is actually processed in the state's benefit system. ETA will provide additional reporting instructions for this workload item in subsequent guidance.

The state will report the initial monetary determination on the ETA 218, Benefit Rights and Experience report. Once the claimant's ID is confirmed, the state must re-issue the monetary determination, with the full employer details. The re-issuance of the monetary determination is not reported on ETA 218, Benefit Rights and Experience report.

Similarly, a monetary denial due to the removal of wages is in essence a monetary redetermination. Redeterminations must not be included in the Benefit Accuracy Measurement (BAM) sample universe and should be deleted from the sample selection.

[2] Note that the alleged victim does not need to verify their own identity for the state to begin an investigation on a suspicious claim. The individual filing the claim is responsible for validating their own identity. If the alleged victim is trying to file a claim, then the state must, as a matter of course in filing a claim, require the alleged victim to validate their own identity.

If these redeterminations are selected in the BAM sampling universe, they must be deleted from the sample. If these monetary redeterminations are consistently included in the BAM sample, ETA strongly recommends that the state agency review and address any inconsistencies within its reports in order to correct this issue.

States would report non-monetary determinations based on the individual's failure to respond to the identity verification request in the ETA 207 Nonmonetary Determination Activities report, on lines 301 and 302, in column 15 "Reporting Requirement Call-ins and Other". The state will report any non-monetary determinations based on the individual's failure to verify identity on the ETA 207 Nonmonetary Determination Activities report on lines 301 and 302, in column 17 "Other (Aliens, Athlete, School)".

Additionally, ETA is creating a new category for ID verification issues and additional reporting instructions for affected UC required reports. Until this new category is created, states must report the number of determinations and denials reported in column 15 and column 17 for failure to report/respond issues and failure to verify identity determinations.

5. <u>Protecting ID Theft Victims</u>.

When a state determines that ID theft has occurred, that is, the person filing the claim is not the actual owner of the name and/or SSN under which the claim was filed, it must take precautions to protect the rights of the ID theft victim and mitigate the negative consequences related to the fraudulent activity, including:

- Ensure that if a future claim is filed under the victim's SSN, the claimant undergoes a secondary ID verification process (e.g., include an in-person reporting requirement or other expanded ID verification alternatives). However states should try to minimize the burden on the victim as much as possible when verifying identity;
- Ensure that the owner of the SSN is not held responsible for any overpayment or, whenever possible, is not issued a Form 1099G at the end of the year;
- Exclude the overpayment from the Treasury Offset Program (TOP) and suspend any Benefit Payment Control collection activity; and
- Not initiating any legal actions against the actual owner of the SSN.

One option states can use to mitigate negative impacts on ID theft victims is to establish a pseudo claim record and transfer all claim information regarding the imposter's claim to the pseudo claim once the state makes a fraud determination. This removes the fraudulent activity from the victim's SSN, should the victim need to file for unemployment benefits in the future. Additionally, this preserves data from the fraudulent activity to be used for future analytics.

States must provide individuals who suspect theft of their identity for purposes of filing UI claims easily accessible options to report such theft or fraudulent activity, such as dedicated phone lines, email addresses or an online portal by which individuals can notify the state agency. States may also provide links to other agencies that specialize in protecting

consumers and their personal identifiable information, such as the Federal Trade Commission's Consumer website at https://www.consumer.ftc.gov/topics/identity-theft. ETA strongly encourages state workforce agencies to align their state website content and communications for victims of unemployment identity theft with the content, resources, and reporting requirements outlined at www.dol.gov/fraud.

6. Cases Selected for Program Integrity/Quality Reviews.

Claims involving ID verification issues that are selected for review through the ongoing BAM program or the Benefit Timeliness and Quality Review (BTQ) program should include the following information in the BAM/BTQ case file in order to complete its analysis or investigation:

- All documentation related to the ID verification processes utilized on the claim;
- Case information for the SSN as well as any information transferred to a pseudo SSN; and
- Fact-finding documentation and logic for the claim determination(s).

State agencies are required to complete BAM coding for ID theft consistent with the methodology outlined in the ETA Handbook No. 395 and the error coding for elements (ei1) through (ei4) must reflect the action taken by the BAM investigator as summarized below:

- (ei1) = the amount paid for the key week;
- (ei2) Key Week Action = 10;
- (ei3) Error Cause = 480 through 489; and
- (ei4) Error Responsibility may include 4 to reflect the person or entity who committed the identity theft.

The prior actions recorded in elements (ei5) BAM Detection Point, (ei6) Prior Agency Action, (ei7) Prior Employer Action, and (ei9) Prior Claimant Action should also be included.

7. Tools Available through the UI Integrity Center Integrity Data Hub (IDH).

As most recently discussed in UIPL Nos. 23-20, 28-20, and 28-20, Change 1, the IDH is a secure, robust, centralized, multi-state data system that allows participating state UI agencies to submit claims for crossmatching and analysis to support the prevention and detection of improper payments, fraud, and ID theft. The IDH contains an expanded set of data sources and new functionality continues to be explored and added. Currently the IDH offers the following capabilities:

- Identity Verification (IDV)
- Suspicious Actor Repository (SAR);
- Suspicious E-Mail Domains;
- Foreign IP Address Detection;
- Multi State Cross-Match (MSCM);

- Data Analytics;
- Fraud Alert System; and

In July 2020, the IDH added an IDV component, which provides centralized ID verification solution. The IDV component offers states advanced ID verification scoring to maximize front-end ID verification, enabling states to assess whether an individual is using a false, stolen, or synthetic ID.

The IDH is available to participating states at no cost and is an effective tool in preventing and detecting improper payments and combatting imposter fraud and ID theft. All states are strongly encouraged to participate.[3]

8. Inquiries. Please direct inquiries to the appropriate ETA Regional Office.

9. References.

- Computer Matching and Privacy Protection Act of 1988 (CMPPA) (5 U.S.C. § 552a(o)-(r));
- Identity Theft and Assumption Deterrence Act of 1998 (18 U.S.C. § 1028 note)
- Section 303 of the Social Security Act (SSA) (42 U.S.C. § 503);
- Claim Determination (CD) Standards set forth at 20 C.F.R. Part 614 Appendix B;
- Standard for Benefit Payment Promptness - Unemployment Compensation, 20 C.F.R. Part 640;
- UIPL No. 28-20, Change 1, *Additional Funding for Identity Verification or Verification of Pandemic Unemployment Assistance (PUA) Claimants and Funding to Assist with Efforts to Prevent and Detect Fraud and Identity Theft as well as Recover Fraud Overpayments in the PUA and Pandemic Emergency Unemployment Compensation (PEUC) Programs*, issued January 15, 2021, https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=9897;
- UIPL No. 28-20, *Addressing Fraud in the Unemployment Insurance (UI) System and Providing States with Funding to Assist with Efforts to Prevent and Detect Fraud and Identity Theft and Recover Fraud Overpayments in the Pandemic Unemployment Assistance (PUA) and Pandemic Emergency Unemployment Compensation (PEUC) Programs*, issued August 31, 2020, https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=8044;
- UIPL No. 23-20, *Program Integrity for the Unemployment Insurance (UI) Program and the UI Programs Authorized by the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020 - Federal Pandemic Unemployment Compensation (FPUC), Pandemic Unemployment Assistance (PUA), and Pandemic Emergency Unemployment Compensation (PEUC) Programs*, issued May 11, 2020, https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=4621;

[3] The Pacific territories (Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, the Federated States of Micronesia, the Republic of the Marshall Islands, and the Republic of Palau) do not have access to the IDH.

- UIPL No. 02-16, Change 1, *State Responsibilities for Ensuring Access to Unemployment Insurance Benefits*, issued May 11, 2020, https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=5491;
- UIPL No. 02-16, *State Responsibilities for Ensuring Access to Unemployment Insurance Benefits*, issued October 1, 2015, https://wdr.doleta.gov/directives/corr_doc.cfm?docn=4233;
- UIPL No. 01-16, Change 1, *Federal Requirements to Protect Individual Rights in State Unemployment Compensation Overpayment Prevention and Recovery Procedures – Questions and Answers*, issued January 13, 2017, https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=7706;
- UIPL No. 01-16, *Federal Requirements to Protect Individual Rights in State Unemployment Compensation Overpayment Prevention and Recovery Procedures*, issued October 1, 2015, https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=5763;
- UIPL No. 04-01, *Payment of Compensation and Timeliness of Determinations during a Continued Claims Series*, issued October 27, 2000, https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=1746;
- UIPL No. 35-95, *The Department of Labor's Position on Issues and Concerns Associated with the Utilization of Telephone and Other Electronic Methods in the Unemployment Insurance (UI) Program*, issued June 28, 1995, https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=1901;[4]
- ET Handbook No. 401, 5th edition, Unemployment Insurance Reports Handbook, August 2017;
- ET Handbook No. 301, 5th edition, UI Performs: Nonmonetary Determinations Quality Review, July 29, 2005;
- Report Unemployment Identity Theft, U.S. Department of Labor Employment and Training Administration website, www.dol.gov/fraud;
- UI Integrity Center website, https://www.naswa.org/integrity-center; and
- Unemployment Insurance Fraud Consumer Protection Guide, U.S. Department of Justice, issued September 21, 2020, https://www.justice.gov/file/1324726/download.

[4] We note that the link to this document shows an expiration date of June 30, 1996. However, per Training and Employment Notice No. 15-20, issued January 14, 2021, this remains an active UIPL.