Memorandum of Agreement
Between
State of Utah Department of Workforce Services
And

(Insert Creditor's Name Here)

DISCLOSURE OF INFORMATION FOR DEBT COLLECTION

A. Purpose

This Agreement is made between the **State of Utah Department of Workforce Services** (hereafter referred to as "DWS") and the **Insert Creditor's Name Here** (hereafter referred to as "Creditor"), in accordance with Utah Code Ann. § 35A-4-314. DWS agrees to disclose certain employment records (hereafter referred to as "RECORDS") to Creditor who has obtained judgment against a debtor and has met all conditions specified in § 35A-4-314. DWS and Creditor may herein be referred to collectively as the "Parties."

B. Background

Historically, DWS could only release RECORDS to creditors who provided DWS with written authorizations signed by all affected parties allowing RECORDS to be released. Utah Code Ann. § 35A-4-314 was amended in the 2013 General Session of the State of Utah to require DWS to disclose RECORDS to Creditors in the event the Creditors meet all of the requirements delineated within the statute. The amendments were signed by the Governor of Utah on April 1, 2013, and went into effect on May 14, 2013.

The Parties agree that when a Creditor meets all requirements specified in Utah Code Ann. § 35A-4-314, DWS will disclose RECORDS to that creditor with the goal of facilitating legal debt collections by that Creditor against their debtors.

C. Period of Performance

This Memorandum of Agreement (MOA) is effective upon the signature of both parties and shall remain in effect for a period of five (5) years or until modified in writing by the mutual consent of both parties or terminated by either party upon 30 days prior written notice to the other party.

D. Termination

DWS may terminate this MOA without prior notice if deemed necessary because of a requirement of law or policy, upon determination by DWS that there has been a breach of system integrity or security by Creditor, or a failure of Creditor to comply with the terms of this Agreement, established procedures, or legal requirements.

E. Attachments Included as Part of this Agreement

Attachment A: Title 35A, Chapter 4, Section 314
Attachment B: 20 C.F.R. Section 603.9

F. Legal Authority

DWS will enter into agreements concerning the disclosure RECORDS with Creditor as required or permitted under the provisions of Utah Code Ann. § 35A-4-314, 20 C.F.R. Part 603, or other applicable law and the rules adopted pursuant thereto.

1. **Wage Records**: The Wagner-Peyser Act, as amended (29 U.S.C § 49 et seq.); the Workforce Investment Act of 1998, 29 U.S.C. § 2801 et seq., P.L. 106-113 (WIA); the Utah Code Ann. § 35A-4-312(5)(e), (i); Unemployment Insurance Program Letter (UIPL) No. 21-99, including Attachments A and B; and 20 C.F.R. § 666.150 definition of "quarterly wage record information" to be used for WIA performance measurement; 20 C.F.R. § 603.9 confidentiality protection provisions.

2. **Social Security Records:** The Privacy Act of 1974, (5 U.S.C. § 552a, as amended); the Social Security Administration Privacy Act Regulations (20 C.F.R. § 401.150, as amended); and the Social Security Act's Disclosure of Information in Possession of an Agency (42 U.S.C. § 1306, as amended).

G. Format and Processing Fees for Creditor Request for RECORDS

Creditor must submit each request in writing, along with the associated court order, for RECORDS to DWS in a format approved by DWS. The court order must be signed and stamped by the court. At the time Creditor submits a request to DWS for RECORDS, Creditor must pay DWS a $15 fee to process Creditor's request for RECORDS. Creditor must pay the $15 fee for RECORDS for each individual debtor search, whether or not DWS has RECORDS being sought by Creditor. If Creditor fails to pay the $15.00 fee to DWS as specified, or if Creditor does not submit the request in the format approved by DWS, DWS will not process Creditor's request for RECORDS.

H. DWS Release of RECORDS to Creditor

If Creditor meets all the requirements of Utah Code Ann. **§** 35A-4-314 and of this Agreement, DWS will return a secure response to Creditor's request for RECORDS within 14 business days in a format approved by DWS.

I. Limitations of Information Provided to Creditor

The specific information requested of each matched RECORD is confirmation of most recent employment information, specifically the employer name and address. Creditor understands that the matching information returned to Creditor has not been verified for accuracy by DWS and is largely information submitted by the employer or employer's agent during periodic submission of Utah UI wage data, and as such, DWS does not provide any assurances of the accuracy of the information provided.

Creditor understands that the information obtained by DWS may only be used for the purpose of satisfying the judgment between the Creditor and debtor and may not be shared or disclosed with any other person.

J. Disclosure and Confidentiality Requirements

1. Creditor shall have sufficient safeguards in place to ensure the information obtained is used only for the purpose disclosed. Information in electronic format shall be stored and processed in such a way that unauthorized persons cannot retrieve the information by computer, by remote terminal, or by any other means.
2. The information shall not be stored on any server accessible from the Internet or by unauthorized Creditor personnel.
3. At the request of DWS, the Creditor shall identify all Creditor personnel, by position, authorized to request and receive information.
4. Creditor shall permit DWS or designee and other authorized state and federal officials to make on-site inspections to ensure that the requirements of this Agreement and state and federal statutes and regulations are being met.
5. Wage Record Confidentiality: Creditor shall follow the confidentiality protections provisions of 20 C.F.R. § 603.9 (*see Attachment B)* until such time as the Secretary of Labor issues new confidentiality regulations. Thereafter, Creditor shall follow the new regulations.
6. Wage Records – Unlawful Access or Disclosure Penalties: Any person who knowingly and willfully requests or obtains wage records under false pretenses, or any person who knowingly and willfully discloses any such information in any manner to any individual not entitled under law to receive it, shall be guilty of a Class A misdemeanor with a sentence of imprisonment not exceeding one year and/or a fine not exceeding $2,500 under Utah law (Utah Code Ann. §§ 76-8-1301(3), 76-3-204(1), and 76-3-301(1)).
7. Social Security Record Confidentiality: The confidentiality of social security records shall be maintained in accordance with 42 U.S.C. § 1306; 5 U.S.C. § 552a; and 20 C.F.R. § 401.150.
8. Re-disclosure of Social Security Record Information: Social security records may only be re-disclosed pursuant to the provisions of 42 U.S.C. § 1306; 5 U.S.C. § 552a; and 20 C.F.R. § 401.150.
9. Social Security – Unlawful Access or Disclosure Penalties: The penalties for unlawful access or disclosure of social security records shall be governed by the provisions of 42 U.S.C. § 1306.
10. Unemployment Insurance Record Confidentiality: The confidentiality of unemployment insurance records shall be maintained pursuant to the provisions of Utah Code Ann. § 35A-4-312; Utah Code Ann. § 63G-2-206; and 20 C.F.R. § 603.9.
11. Re-disclosure of Unemployment Insurance Record Information: Unemployment insurance records may only be re-disclosed pursuant to the provisions of Utah Code Ann. § 35A-4-312; Utah Code Ann. § 63G-2-206 and 20 C.F.R. Part 603.
12. Unemployment Insurance – Unlawful Access or Disclosure Penalties: The penalties for unlawful access or disclosure of unemployment insurance records by Creditors who receive the information from the Department shall be governed by the provisions of Utah Code Ann. § 35A-4-314.

K. Data Security

Creditor shall monitor, detect, analyze, protect, report, and respond against known vulnerabilities, attacks, and exploitations. Creditor shall also continuously test and evaluate information security controls and techniques to ensure that they are effectively implemented.

1. **Background Checks:** Creditor will ensure that it has thoroughly investigated the employees who are given access to this data. "Thoroughly Investigated" includes using the Social Security Number (SSN), date of birth, all known names and/or aliases, and using a national background check program (i.e. BCI) for background checks of the person granted access to the RECORDS. Creditor will not grant access to employees whose background suggests they will be unable to meet the data security requirements of this agreement, including, but not limited to, employees whose background checks reveal fraud or identity theft Background checks should be performed at least every five (5) years. Creditor shall provide documentation of background checks to DWS upon request.
2. **Access to Data:** Creditor shall control access based on need to know. Creditor shall limit access to data in electronic or hardcopy format to authorized individuals only. DWS reserves the right to disapprove access to selected individuals or groups of individuals.
3. **Query Log:** DWS will create and maintain a query log containing the user identification, the date/time of each query, and the Social Security Number used in each query.
4. **Unauthorized Access to Stored Data:** Information either in electronic format such as magnetic tapes or discs or in hardcopy paper format shall be stored and/or processed in such a manner that unauthorized access is avoided. Creditor shall secure data in a manner to protect internal confidential files.
5. **User Training:** DWS and Creditor agree to train users accessing, disclosing, or receiving information under this MOA, including contractors and contract providers, on relevant statutes prescribing confidentiality and safeguarding requirements, re-disclosure prohibitions, and penalties for unauthorized access or disclosure. DWS or designee reserves the right to review disclosure-training programs provided for Creditor employees and require any changes necessary to said programs. Training should take place annually. Creditor shall provide documentation of training to DWS upon request.

   Subsection 35A-4-314(7) of the Utah Employment Security Act provides that

   > *(7) If a judgment creditor or other party fails to comply with the data safeguard and security measures under 20 C.F.R. Sec. 603.9, the judgment creditor or other party is subject to a civil penalty of no more than $10,000 enforceable by the Utah Office of the Attorney General as follows:*
   >
   > *(a) the attorney general, on the attorney general's own behalf or on behalf of the division, may file an action in district court to enforce the civil penalty; and*

(b) if the attorney general prevails in enforcing the civil penalty against the judgment creditor or other party:

(i) the attorney general is entitled to an award for reasonable attorney fees, court costs, and investigative expenses; and

(ii) the civil penalty shall be deposited into the special administrative expense account described in Subsection 35A-4-506(1).

6. **Security Plans:** Creditor system security plans must include provisions warning of the potential statutory sanctions for individuals who violate access and disclosure provisions. Procedures governing sanctions and individual corrective actions under applicable statutory authority shall be pursued and taken against individuals who violate terms of this agreement.
7. **On-site Review:** Creditor shall permit DWS or designee the right of on-site inspection without prior notification to ensure that the requirements of this agreement are being met. Additionally, the Creditor will allow on-site inspections by any other state and federal agencies with statutory oversight responsibility for the data being shared.
8. **RECORDS Retention:** Creditor shall maintain RECORDS for no longer than five (5) years.
9. Creditor shall report any breaches of access and disclosure requirements to DWS within 24 hours.
10. Creditor shall develop a contingency plan for addressing unauthorized access to any sensitive RECORDS.
11. Creditor shall notify DWS of any major change in a system platform (hardware and/or software) procedure and or policy affecting transmission and/or distribution so that re-review of system safeguards can be initiated.
12. Creditor shall comply with the following measures to prevent security breaches. Failure to meet the requirements will result in liability against the Creditor. All workstation updates must be installed within 72 hours of the patch/software/service pack release dates. All server patches/software updates/service packs must be installed within two weeks of release date or within a reasonable time frame, based on professional information technology industry standards and best practices:
    a. Install the most recent OS service pack;
    b. Install the most recent OS security updates;
    c. Install most recent patches for applications including, but not limited to, Adobe (Acrobat, PDF, Reader, Flash), Java, Quick-Time, and Microsoft Office;
    d. Install, run, and maintain anti-virus and anti-malware (computer contaminant) software with the latest signature which includes, but is not limited to, protection from computer viruses, worms, Trojan horses, malicious rootkits, backdoors,

spyware, botnets, keystroke loggers, data-stealing malware, dishonest adware, crimeware, and other malicious software;

e. Maintain secure configurations for hardware and software on laptops, workstations, and servers;

f. Maintain secure configurations on network devices such as firewalls, routers, and switches;

g. Install and maintain adequate boundary defense. Run and maintain Windows Firewall on all devices;

h. Educate and require computer users to put in place strong authentication credentials and passwords;

i. Control wireless devices used to access, transmit, and/or store DWS data. This includes, but is not limited to, the use of:

    i. enterprise management tools (vs. tools for home use);

    ii. network vulnerability scanning tools;

    iii. deactivation of unauthorized ports;

    iv. wireless intrusion detection systems (WIDS);

    v. disabling peer-to-peer network capability;

    vi. disabling wireless peripheral access, such as Bluetooth; and

    vii. disabling the ability to connect to public wireless networks and those not authorized by Creditor.

j. Maintain, monitor and analyze security audit logs;

k. Maintain controlled used of administrative privileges;

l. Continually assess vulnerability and remediate any issues;

m. Limit and control network ports, protocols, and services; and

n. Data Loss Prevention: Prevent data loss through the use of appropriate measures, including but not limited to: encryption software, network monitoring tools, monitoring, and an adequate Data Security Plan and employee training on such plan.

L. Indemnification Clause

Creditor agrees to indemnify, hold harmless, and release the State of Utah and all its officers, agents, volunteers, and employees from and against any and all loss, damages, injury, liability, suits, and proceedings arising out of the performance of this Agreement that are caused in whole or in part by the negligence of the Creditor officers, agents, volunteers, or employees, but not for claims arising from the State's sole negligence.

Contacts

Creditor	***DWS***
	Kathleen Bounous Director of Adjudication/Appeals General Counsel Department of Workforce Services 140 East 300 South Salt Lake City, UT 84111 801-526-9653 kbounous@utah.gov

This MOA, its attachments, and all documents incorporated by reference constitute the entire agreement between the parties and supersede all prior negotiations, representations, or agreements, either written or oral between the parties relating to the subject matter of this MOA.

SIGNATURE AND ACKNOWLEDGEMENT:
By Signing below, the following officials acknowledge that they understand and agree to all of the terms and responsibilities set forth herein and cause this Agreement to be executed.

ATTEST: **Insert Creditor Name Here**

Creditor Signature Date

Print Name and Title

ATTEST: **UTAH DEPARTMENT OF WORKFORCE SERVICES**

Kathleen Bounous, Date
Director of Adjudication/Appeals, General Counsel

ATTACHMENT A

Title 35A Chapter 4 Section 314

Title 35A Utah Workforce Services Code

Chapter 4 Employment Security Act

Section 314 Disclosure of information for debt collection -- Court order -- Procedures -- Use of information restrictions -- Penalties.

(1) The division shall disclose to a creditor who has obtained judgment against a debtor the name and address of the last known employer of the debtor if:

(a) the judgment creditor obtains a court order requiring disclosure of the information as described in Subsection (2); and

(b) the judgment creditor completes the requirements described in Subsection (3), including entering into a written agreement with the division.

(2) (a) A court shall grant an order to disclose the information described in Subsection (1) if, under the applicable Utah Rules of Civil Procedure:

(i) the judgment creditor files a motion with the court, which includes a copy of the judgment, and serves a copy of the motion to the judgment debtor and the division;

(ii) the judgment debtor and the division have the opportunity to respond to the motion; and

(iii) the court denies or overrules any objection to disclosure in the judgment debtor's and the division's response.

(b) A court may not grant an order to disclose the information described in Subsection (1), if the court finds that the division has established that disclosure will have a negative effect on:

(i) the willingness of employers to report wage and employment information; or

(ii) the willingness of individuals to file claims for unemployment benefits.

(c) The requirements of Subsection 63G-2-202(7) and Section 63G-2-207 do not apply to information sought through a court order as described in this section.

(3) If a court order is granted in accordance with this section, a judgment creditor shall:

(a) provide to the division a copy of the order requiring the disclosure;

(b) enter into a written agreement with the division, in a form approved by the division;

(c) pay the division a reasonable fee that reflects the cost for processing the request as established by department rule; and

(d) comply with the data safeguard and security measures described in 20 C.F.R. Sec. 603.9 with respect to information received from the division under this section.

(4) If a judgment creditor complies with Subsection (3), the division shall provide the information to the judgment creditor within 14 business days after the day on which the creditor complies with Subsection (3).

(5) A judgment creditor may not:

(a) use the information obtained under this section for a purpose other than satisfying the judgment between the creditor and debtor; or

(b) disclose or share the information with any other person.

(6) The division may audit a judgment creditor or other party receiving information under this section for compliance with the data safeguard and security measures described in 20 C.F.R. Sec. 603.9.

(7) If a judgment creditor or other party fails to comply with the data safeguard and security measures under 20 C.F.R. Sec. 603.9, the judgment creditor or other party is subject to a civil penalty of no more than $10,000 enforceable by the Utah Office of the Attorney General as follows:

(a) the attorney general, on the attorney general's own behalf or on behalf of the division, may file an action in district court to enforce the civil penalty; and

(b) if the attorney general prevails in enforcing the civil penalty against the judgment creditor or other party:

(i) the attorney general is entitled to an award for reasonable attorney fees, court costs, and investigative expenses; and

(ii) the civil penalty shall be deposited into the special administrative expense account described in Subsection 35A-4-506(1).

Enacted by Chapter 473, 2013 General Session

ATTACHMENT B

20 CFR PART 603—FEDERAL-STATE UNEMPLOYMENT COMPENSATION (UC) PROGRAM; CONFIDENTIALITY AND DISCLOSURE OF STATE UC INFORMATION

§ 603.9 What safeguards and security requirements apply to disclosed information?

(a) *In general* . For disclosures of confidential UC information under § 603.5(d)(2) (to a third party (other than an agent) or disclosures made on an ongoing basis); § 603.5(e) (to a public official), except as provided in paragraph (d) of this section; § 603.5(f) (to an agent or contractor of a public official); § 603.6(b)(1) through (4), (6), and (7)(i) (as required by Federal UC law); and § 603.22 (to a requesting agency for purposes of an IEVS), a State or State UC agency must require the recipient to safeguard the information disclosed against unauthorized access or redisclosure, as provided in paragraphs (b) and (c) of this section, and must subject the recipient to penalties provided by the State law for unauthorized disclosure of confidential UC information.

(b) *Safeguards to be required of recipients* . (1) The State or State UC agency must:

(i) Require the recipient to use the disclosed information only for purposes authorized by law and consistent with an agreement that meets the requirements of § 603.10;

(ii) Require the recipient to store the disclosed information in a place physically secure from access by unauthorized persons;

(iii) Require the recipient to store and process disclosed information maintained in electronic format, such as magnetic tapes or discs, in such a way that unauthorized persons cannot obtain the information by any means;

(iv) Require the recipient to undertake precautions to ensure that only authorized personnel are given access to disclosed information stored in computer systems;

(v) Require each recipient agency or entity to:

(A) Instruct all personnel having access to the disclosed information about confidentiality requirements, the requirements of this subpart B, and the sanctions specified in the State law for unauthorized disclosure of information, and

(B) Sign an acknowledgment that all personnel having access to the disclosed information have been instructed in accordance with paragraph (b)(1)(v)(A) of this section and will adhere to the State's or State UC agency's confidentiality requirements and procedures which are consistent with this subpart B and the agreement required by § 603.10, and agreeing to report any infraction of these rules to the State UC agency fully and promptly,

(vi) Require the recipient to dispose of information disclosed or obtained, and any copies thereof made by the recipient agency, entity, or contractor, after the purpose for which the information is disclosed is served, except for disclosed information possessed by any court. Disposal means return of the information to the disclosing State or State UC agency or destruction of the information, as directed by the State or State UC agency. Disposal includes deletion of personal identifiers by the State or State UC agency in lieu of destruction. In any case, the information disclosed must not be retained with personal identifiers for longer than such period of time as the State or State UC agency deems appropriate on a case-by-case basis; and

(vii) Maintain a system sufficient to allow an audit of compliance with the requirements of this part.

(2) In the case of disclosures made under § 603.5(d)(2) (to a third party (other than an agent) or disclosures made on an ongoing basis), the State or State UC agency must also—

(i) Periodically audit a sample of transactions accessing information disclosed under that section to assure that the entity receiving disclosed information has on file a written release authorizing each access. The audit must ensure that the information is not being used for any unauthorized purpose;

(ii) Ensure that all employees of entities receiving access to information disclosed under § 603.5(d)(2) are subject to the same confidentiality requirements, and State criminal penalties for violation of those requirements, as are employees of the State UC agency.

(c) *Redisclosure of confidential UC information.* (1) A State or State UC agency may authorize any recipient of confidential UC information under paragraph (a) of this section to redisclose information only as follows:

(i) To the individual or employer who is the subject of the information;

(ii) To an attorney or other duly authorized agent representing the individual or employer;

(iii) In any civil or criminal proceedings for or on behalf of a recipient agency or entity;

(iv) In response to a subpoena only as provided in § 603.7;

(v) To an agent or contractor of a public official only if the person redisclosing is a public official, if the redisclosure is authorized by the State law, and if the public official retains responsibility for the uses of the confidential UC information by the agent or contractor;

(vi) From one public official to another if the redisclosure is authorized by the State law;

(vii) When so authorized by Section 303(e)(5), SSA, (redisclosure of wage information by a State or local child support enforcement agency to an agent under contract with such agency for purposes of carrying out child support enforcement) and by State law; or

(viii) When specifically authorized by a written release that meets the requirements of § 603.5(d) (to a third party with informed consent).

(2) Information redisclosed under paragraphs (c)(1)(v) and (vi) of this section must be subject to the safeguards in paragraph (b) of this section.

(d) The requirements of this section do not apply to disclosures of UC information to a Federal agency which the Department has determined, by notice published in the FEDERAL REGISTER, to have in place safeguards adequate to satisfy the confidentiality requirement of Section 303(a)(1), SSA.