



Department of Social Services

Human Resources Administration

Department of Homeless Services

(FOR HRA/DHS INTERNAL USE ONLY)

Office of Legal Affairs
Commercial Law Division

**Approval Signatures and Routing Form For
Memorandum of Understanding (MOU), Cooperative Agreement (CA), and
Intra-City Agreement (ICA)**

Steven Banks
Commissioner

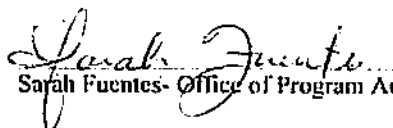
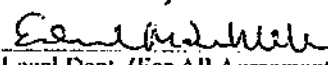
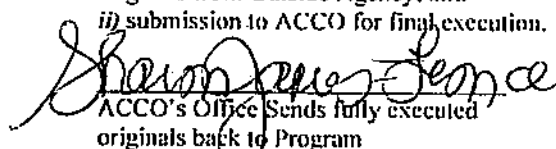
Martha A. Calhoun
General Counsel

Edward M. LeMelle
Senior Deputy
General Counsel

150 Greenwich St
New York, NY 10007

929 221 6461

Parties: State of New York Office of Temporary and Disability Assistance ("OTDA")
Human Resources Administration ("HRA")
Term: From effective date until terminated
Purpose: The State of New York Office of Temporary and Disability Assistance (OTDA) and the New York City Department of Social Services Human Resources Administration (HRA) are entering into this Memorandum of Understanding (MOU), relative to the sharing of information from the OTDA Specialized Fraud and Abuse Reporting System (SFARS) to further strengthen HRA trafficking detection efforts in the Supplemental Nutrition Assistance Program (SNAP).

- | | | <u>Date</u> |
|---------|---|-------------|
| Step 1. |  Sarah Fuentes - Office of Program Accountability | 9/26/19 |
| Step 2. | Finance Office (with financial impact) (Erin Villari - 150 Greenwich St., 34 th Fl.) | |
| Step 3. | Legal Dept (For D/S MOUs Only) (Aaron Goodman - 150 Greenwich St., 38 th Fl.) | |
| Step 4. |  Legal Dept. (For All Agreements) (Edward LeMelle - 150 Greenwich St., 37 th Fl.) | 9/26/19 |
| Step 5. | Program Sends 5 Originals to Outside Agency for Execution | |
| Step 6. | Program Signature indicating i) Receipt of five (5) signed and notarized originals from Outside Agency; <i>and</i> ii) submission to ACCO for final execution. | |
| Step 7. |  ACCO's Office Sends fully executed originals back to Program (150 Greenwich St., 37 th Fl.) | 11/18/19 |
| Step 8. | Program Sends 2 Fully Executed Originals To Outside Agency | |

Program Area: Inna Brenayzen- IREA/OPA
Phone: 929-252-2715

**Memorandum of Understanding between the State of New
York Office of Temporary and Disability Assistance and the
New York City Department of Social Services Human
Resources Administration**

The State of New York Office of Temporary and Disability Assistance (OTDA) , its employees, officers, agents, HRAs, subcontractors, and/or other representatives and the New York City Department of Social Services Human Resources Administration (HRA) are entering into this Memorandum of Understanding (MOU) dated 07/26/2019, relative to the sharing of information from the OTDA Specialized Fraud and Abuse Reporting System (SFARS) to further strengthen HRA trafficking detection efforts in the Supplemental Nutrition Assistance Program (SNAP).

In connection with this Agreement, HRA will receive, have access to, or be exposed to certain documents, records, and other information (including electronically stored information), that is Protected Information as defined under the Definitions sections of this Agreement and protected from disclosure, including, but not limited to: records sufficient to identify an applicant for, or recipient of, SNAP benefits; personally identifiable information (PII) such as social security number, name and date of birth, information on authorized SNAP retailers, as well as other records, reports, information, and statements required to be protected by federal or State laws, regulations, or by court order. Specific data elements included are contained in Appendix A.

In consideration of the mutual promises and covenants contained herein, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. HRA will only use the documents, records, and other information (including electronically stored information) pursuant to this agreement through SFARS to investigate public benefits fraud and SNAP trafficking through investigations and data analytics.
2. HRA will not use the SBU or PII Information for its personal purposes or benefit, and will not release or reveal any City, State or Federal protected information outside of the agreed upon terms and conditions of this MOU.
3. At the conclusion of this project, HRA will purge all State provided Information in its custody or control, in the manner required by the State and outlined in this MOU.
4. This MOU can be terminated at any time by either party, with or without cause. Upon termination of the agreement, any restrictions contained herein as to the State Information and/or the HRA shall survive indefinitely.

Information Security, Privacy, Confidentiality and Compliance

This Section shall apply when Protected Information (as defined below) is stored, used, accessed or obtained by HRA.

A. Definitions:

For purposes of this Section the following terms shall have the following meanings:

"Protected Information" means data or information to which the HRA is given access which OTDA creates, receives, or maintains, which is, pursuant to federal and/or state laws, rules, regulations, policies or agreements, deemed confidential, personal, private and/or sensitive. Such data or information may be present or stored in any form or medium and includes, but is not limited to:

1. Data or information obtained from sources outside of OTDA;
2. Data or information maintained in and/or obtained from OTDA-owned applications, systems, networks and/or databases; Data or information identifying an individual, particularly where such disclosure could result in unwarranted invasion of personal privacy;
3. Computer codes or other electronic or non-electronic data or information, the disclosure of which could jeopardize the compliance stature, security or confidentiality of OTDA's information technology solutions, applications, systems, networks or data;
4. Any other material designated by OTDA as being "Confidential," "Personal," "Private," or otherwise "Sensitive."

"Authorized Persons" means HRA's employees, subcontractors or other agents who are authorized and have a business justification to access Protected Information to enable HRA to perform the services pursuant to the Agreement.

"Information Security Incident" means any allegation or suspicion held by or brought to the attention of an OTDA employee or Authorized Persons involving inappropriate or unauthorized access to, or disclosure of, Protected Information.

"Information Security Breach" means the unauthorized access by a non-Authorized Person of Protected Information as defined in New York State Information and Security Breach Notification Act (General Business Law Section 899-aa; State Technology Law Section 208).

"OTDA Contact" means the person or persons designated in writing by OTDA to receive Information security incident or Information security breach notifications.

"Continental United States (CONUS)" – the 48 contiguous States and the District of Columbia

"Follow the Sun" – Follow-the-sun is a type of global workflow in which tasks are passed around daily between work sites that are many time zones apart. All helpdesk, online, and support services which access any Data must be performed from within CONUS.

B. Data to be Disclosed:

A list of the specific information to be furnished by OTDA to HRA under this agreement is included in Appendix A. This information is hereinafter referred to as Protected Information.

C. Purpose of Data:

HRA represents that it is requesting Protected Information solely for purposes of investigating public benefits fraud and trafficking in the Supplemental Nutrition Assistance Program (SNAP). Analyzing this data will inform client and retailer fraud and trafficking investigations by HRA alone, or in conjunction with law enforcement agencies and the United States Department of Agriculture (USDA). OTDA will release Protected Information to HRA exclusively for this purpose. HRA shall use the Protected Information only for the authorized purposes specified in this agreement.

D. Ownership of Data:

HRA agrees that OTDA shall be deemed the "owner" of Protected Information disclosed by OTDA to HRA under this Agreement solely for purposes of complying with the requirements of State Technology Law Section 208.

E. Data Exchange Details:

Prior to OTDA's sharing of any data pursuant to this agreement, HRA and OTDA shall work together to provide and establish a secure, encrypted (both in transit and at rest) method of data exchange for any transfer of such data which shall, at a minimum, comport with the standards set and required by the New York State Enterprise Information Security Office (NYS EISO) and, where required, any additional heightened compliance obligations applicable to and necessitated by the data involved in any such exchange. The NYS EISO's office shall, as OTDA deems appropriate, be provided with details of such proposed method of exchange for review and approval. a Technical Service Description.

Under this Agreement the data is to be exchanged is as follows:

On a weekly basis, OTDA will use a secured FTP (sFTP) service to transmit a file of all completed cash assistance and Supplemental Nutrition Assistance Program (SNAP) transactions received from the EBT vendor during the prior week for HRA clients. See **Appendix A** for a description of the data content of the file.

F. Data Protection:

Safeguarding of Protected Information shall be an integral part of the business requirements and activities of HRA to ensure there is no inappropriate or unauthorized use or exposure of Protected Information at any time. HRA shall safeguard the confidentiality, integrity and availability of Protected Information and comply with the following conditions:

(i) Implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure, or theft of Protected Information. Such security measures shall comply with industry best practices and shall, at a minimum, comply with those requirements set forth by the NYS Enterprise Information Security Office, and must comply with all applicable state and federal law, rules, regulations and policies.

(ii) All Protected Information shall be encrypted at rest and in transit, in accord with, at a minimum, the standard set forth by the NYS Enterprise Information Security Office, all applicable state and federal law, rules, regulations and policies and, as appropriate, industry best practices.

(iii) At no time shall any Protected Information be copied, disclosed or retained by the HRA for any purpose other than performing the services under this Agreement.

(iv) HRA and Authorized Persons shall not disseminate, use, or permit the dissemination or use of Protected Information in any manner not described in this Agreement without express prior written consent from OTDA.

(v) Host all Protected Information and maintain and implement procedures to logically segregate and secure Protected Information from HRA's data and data belonging to HRA's other customers, including other governmental entities.

(vi) All data will be protected in transit and at rest.

(vii) HRA carefully, thoroughly, and thoughtfully vets the software solutions used to verify that they are compliant with the requirements set forth by the NYS Enterprise Information Security Office and fulfill the compliance obligations for the protection of OTDA's Protected Information. This vetting process shall also extend to any software solutions used by Authorized Persons.

(viii) At no time will any Follow the Sun support be allowed to access Data directly, or indirectly, from outside CONUS.

G. Data Security:

HRA shall immediately disclose its non-proprietary security processes and technical limitations to OTDA such that adequate protection for Protected Information is attained. At a minimum HRA represents and warrants that the security requirements and processes shall comport with the security standards and protocols set by the New York State Enterprise Information Security Office. In addition, HRA shall also comply with any state and/or federal laws, rules, regulations and/or policies that are applicable to the data being exchanged under this Agreement, including any heightened compliance obligations. The system and procedure that HRA will maintain for handling, storage, use, and destruction of Protected Information governed by this agreement will be sufficient to allow OTDA and/or their designee(s) to audit compliance with this Agreement.

H. Data Location:

HRA shall provide its services solely from data centers physically located within the continental United States (CONUS), meaning the 48 contiguous States and the District of Columbia. Storage of Protected Information at rest shall be located solely in data centers in the CONUS. HRA shall not store, access, maintain or process Protected Information on a mobile or portable device. HRA will store and maintain Protected Information in a place and manner that is physically secure from access by unauthorized persons (e.g., locked cabinets or storage room) and will store and process electronic Protected Information in such a way that unauthorized persons cannot obtain the information by any means.

I. Contract and Data Center Audit:

HRA shall allow OTDA and any other authorized government agency to audit HRA's compliance with the security procedures set forth in this section. HRA shall perform an independent audit of its data centers which contain Protected Information at least annually, and provide OTDA a copy of such audit report. Any deficiencies identified in the audit report or where HRA is found to be noncompliant with Agreement safeguards, must be remedied, within 90 days of the issue date of the audit report with proof of remediation provided to OTDA. The completion of this requirement is at HRA's expense with no additional cost to OTDA.

HRA will maintain a system and/or procedures for the handling, storage, use, and destruction of Protected Information governed by this Agreement sufficient to allow OTDA and/or their designee(s) to audit compliance with this Agreement.

HRA will permit OTDA, or their agent, to enter upon HRA's premises at reasonable times to inspect and review their safeguards and procedures for protecting the confidentiality and limiting dissemination of confidential information. HRA will also cooperate with OTDA, or their agent, in connection with any request for access to staff, information, or material related to an OTDA confidentiality compliance review, audit, or monitoring visit.

HRA will provide, at HRA's expense, an independent third-party audit of all data center(s) used to perform the services under the resulting Contract showing no deficiencies. Thereafter on an annual basis, at the HRA's expense, a full version of the audit report will be provided to the State, within 30 days of the anniversary date of the Agreement. A Service Organization Control (SOC) 2 Type 2 audit report or approved equivalent sets the minimum level of a third-party audit.

J. Access:

HRA will limit access to Protected Information to the authorized employees of the Office of Program Accountability and NYC DSS Information Technology Systems (ITS), or their successors in such position, who have are involved in administration or enforcement of the Food and Nutrition Act of 2008. HRA will advise OTDA in writing of changes to the group authorized to perform those duties. Notice of such change will be sent to:

OTDA General Counsel
40 North Pearl Street 16C
Albany, NY 12243
(518) 474-9502
Otda.sm.iso@otda.ny.gov

Neither party may assign or subcontract the Agreement, its obligation or any interest hereunder, without express, prior written consent of the other party. Any assignment or subcontract made without such consent will be null and void and would constitute grounds for immediate termination of the Agreement by OTDA.

HRA expressly represents and agrees that it will not re-disclose Protected Information provided by OTDA under this agreement to third parties, including contractors, without prior written approval from OTDA. HRA employees shall not disseminate, use, or permit the dissemination or use of Protected Information in any manner not provided for in this agreement without express prior written consent from OTDA.

HRA will undertake precautions to limit access to disclosed Protected Information to authorized persons only. HRA will adopt safeguards and procedures to limit dissemination only to authorized individuals with a legitimate business need/purpose related to the purpose of this agreement as set forth in this Agreement.

K. Training:

HRA will ensure that all Authorized Persons who have access to any Protected Information for authorized purposes set forth in this Agreement have been instructed in a manner approved by OTDA regarding the confidential nature of the Protected Information, the safeguards required to protect such data, and the sanctions in applicable state and federal law for unauthorized disclosure of Protected Information. HRA will annually sign an acknowledgement that all Authorized Persons with access to Protected Information have been instructed in a manner approved by and as set out above. HRA will provide this acknowledgement upon request to OTDA and prior to the disclosure of any Protected Information hereunder and annually as required to continue the disclosure of Protected Information hereunder.

HRA and Authorized Persons who have access to Protected Information shall comply with the limitations on data use, access, disclosure, privacy, and security set forth in this Agreement. Such steps will include, but not be limited to, requiring each individual with access to Protected Information to acknowledge in writing that he/she understands and will comply with such limitations.

L. Confidentiality Agreements:

HRA shall require subcontractors to sign a confidentiality and non-disclosure agreement in relation to Protected Information with such non-disclosure agreement attached here in as Appendix B. Such signed agreements must be obtained prior to Authorized Persons commencing work. HRA shall maintain such agreements for the duration of this Agreement and for the duration of any state or federal laws, rules, regulations and policies applicable to the Protected Information being exchanged under this Agreement, whichever is longer, and shall provide them to OTDA upon request.

M. Notification of Legal Requests:

HRA shall immediately inform OTDA in writing upon receipt of any legal, investigatory, or other mode or method of demand (including but not limited to FOIL or FOIA requests, electronic discovery, litigation holds, and discovery searches) for access to Protected Information that is not otherwise authorized under this Agreement and shall take and vigorously pursue all necessary legal action to prevent any disclosure including, but not limited to, moving to quash subpoenas issued for such information. HRA will keep OTDA's General Counsel fully and timely notified of all developments related to such legal actions and their response thereto, and provide appropriate, robust legal assistance as may be required, as requested by OTDA. The notification shall be directed to:

OTDA General Counsel
40 North Pearl Street 16 C
Albany, NY 12243
(518) 474-9502
Otda.sm.iso@otda.ny.gov

N. Report or Publication:

HRA will ensure that any study, report, publication, or other disclosure of Protected Information provided under this Agreement is limited to the reporting of aggregate data, and will not contain any information identifiable to a private person or entity.

O. Return/Destruction of Protected Information:

In the event of termination or expiration of the Agreement, HRA shall, if OTDA requires same, immediately implement an orderly return of all Protected Information, whether in digital or any other form, in a mutually agreeable format at a time agreed to by the parties, but in no event later than 30 days from the date of termination. Thereafter, HRA shall, unless otherwise advised in writing by OTDA, immediately destroy and/or sanitize, as appropriate to the medium, such data and any extracts, copies, or backups of same thoroughly and irretrievably. The method for the sanitization of data shall, at a minimum, comport with the standards set by the New York State Enterprise Information Security Office for the sanitization of data. HRA shall thereafter certify in writing and provide proof that these actions have been completed within 30 days of termination or expiration of this Agreement or within 7 days of the request of an agent, employee or officer of OTDA, at the discretion of OTDA. HRA will not make, retain, copy, duplicate, or otherwise use any copies of Protected Information after completion of the purpose for which the data disclosed is served without prior written permission from OTDA.

P. Data Retention:

Notwithstanding any other obligation under this Agreement, HRA agrees that it will preserve the Protected Information in a manner that complies with all applicable federal and state laws, rules, regulations and policies pertaining to the applicable data records retention.

Q. Compliance with Information Security Breach Notification Act and other Laws:

HRA agrees to abide by all requirements for protecting SNAP client and retailer data as required by the Food and Nutrition Act. HRA represents and warrants that its collection, access, use, storage, disposal and disclosure of Protected Information does and will comply with all applicable federal and state privacy, confidentiality, security, data protection and compliance laws, rules, regulations, policies and directives. HRA warrants that it will comply with the New York State Information and Security Breach Notification Act (General Business Law Section 899-aa; State Technology Law Section 208). HRA ensures that it and all Authorized Persons will be in compliance with the aforementioned state and federal laws, rules, regulations policies and directives.

R. Vulnerability Scanning:

HRA must perform appropriate and required environment vulnerability scanning in accordance Industry best practices and standards. HRA must promptly provide such scan results to OTDA and address all high and medium vulnerabilities found during scanning in a reasonable timeframe as agreed upon with OTDA.

When software vulnerabilities are revealed and addressed by a vendor patch, HRA will obtain the patch from the applicable vendor and categorize the urgency of application as either "critical" or "non-critical" in nature. The determination of the critical versus non-critical nature of patches is solely at the reasonable discretion of OTDA in consultation with NYS ITS and HRA. HRA will apply all critical security patches, hot fixes, or service packs as they are tested and determined safe for installation after consultation with OTDA and NYS ITS.

S. Information Security Incident and Information Security Breach:

If HRA or any Authorized Person or subcontractor becomes aware of or has knowledge of either any potential Information Security Incident (Security Incident) or Information Security Breach (Security Breach), HRA shall as soon as becoming aware, but in no event more than 24 hours, of any potential Security Incident or Security Breach, notify the OTDA contact listed below of the Security Incident or Security Breach via the email address noted, and OTDA will direct what further action is necessary in response to same. At such time, HRA shall provide OTDA with the name and contact information for an employee of HRA who shall serve as HRA's primary security contact and shall be available to assist OTDA twenty-four (24) hours a day, seven (7) days per week in keeping OTDA fully and timely notified of all developments relating to any such potential or actual Security Incident or Security Breach utilizing the following contact information:

OTDA General Counsel
40 North Pearl Street 16 C
Albany, NY 12243
(518) 474-9502
Otda.sm.iso@otda.ny.gov

Should an Information Security Incident or Security Breach occur, immediately following the requisite notification to OTDA, HRA shall 1) promptly investigate and utilize best efforts and IT industry best practices to determine the cause(s) of and devise a proposed resolution and report the causes and suggested remedies to OTDA; (2) promptly implement necessary remedial measures as OTDA and HRA agree as being deemed necessary; (3) document responsive actions taken, including any post-incident review of events and actions taken to make changes in business practices to prevent similar instances in the future; 4) provide reports within the timeframes as requested by OTDA; 5) promptly notify OTDA of the steps taken to prevent similar instances in the future; and 6) take any other action as may be directed by OTDA.

Notification and Assistance to Affected Persons.

HRA shall be responsible for:

- a) promptly notifying individuals whose Protected Information was compromised by an Information Security Breach ("Affected Persons") or, as appropriate, an Information Security Incident. HRA is to first seek consultation and receive authorization from OTDA prior to issuing such notifications. OTDA shall approve the content of and the method by which such notifications must be provided (e.g., regular mail, e-mail, and/or website posting);

- b) providing mitigating services to Affected Persons as mutually agreed upon by OTDA and HRA as reasonably necessary pursuant to a risk analysis of the Information Security Breach. Such services may include, but are not limited to, credit monitoring services, identity theft consultation and restoration, identity theft insurance, public records monitoring, toll free number and call center, and payday loan monitoring (together referred to as “Affected Persons Assistance”);

HRA Responsible for Costs. HRA shall bear all costs associated with providing Affected Persons Assistance. OTDA may reduce any HRA invoice by an amount attributable to HRA’s failure to satisfactorily provide Affected Persons Assistance.

T. Suspension/Termination:

OTDA agrees to provide Protected Information pursuant to this Agreement subject to the representations and agreements by HRA contained in this document. OTDA will suspend the Agreement and the further disclosure of any Protected Information hereunder if: (i) HRA fails to comply with any provision of this Agreement or (ii) OTDA General Counsel believes in good faith that the HRA has violated its obligations to maintain the confidentiality, privacy, security and/or compliance status of such data or limit properly limit dissemination of such data. Such suspension will continue until corrective action, approved by OTDA, has been taken. In the absence of prompt and satisfactory corrective action, OTDA may, at its sole discretion, terminate the Agreement. Upon termination, HRA must immediately return all Protected Information obtained by the HRA or Authorized Persons under the Agreement pursuant to the terms and conditions of the Return/Destruction of Protected Information section within this Agreement.

U. General Terms:

In addition to suspension or termination of the Agreement as provided herein, OTDA reserves the right to undertake, without limitation, any other action under the Agreement, or state or federal law, rule, or regulation, to enforce the Agreement and secure satisfactory corrective action and/or return and/or destruction of the Protected Information furnished hereunder, including seeking damages, penalties, and restitution from HRA or its affiliates as permitted under law.

HRA’s and Authorized Person’s confidentiality and related assurances and obligations hereunder shall survive the termination or expiration of the Agreement.

V. Assignment or Subcontracting:

HRA may not assign or subcontract the obligations or interests outlined in this Section of this Agreement, without express, prior written consent of OTDA. Any assignment or subcontract made without such consent will be null and void and shall constitute grounds for immediate termination of the Agreement by OTDA.

W. Notice:

Any notice required or permitted under this Agreement will be effective upon delivery by certified mail, return receipt requested, or by an overnight courier service that provides written proof of delivery. All notices shall be sent to the following addresses, subject to a Party changing its address from time to time upon written notice to the other Party:

If to OTDA:

OTDA General Counsel
40 North Pearl Street 16C
Albany, NY 12243
(518) 474-9502
otda.sm.iso@otda.ny.gov

If to HRA:

Chief Data Privacy Officer
Office of Legal Affairs
150 Greenwich Street, 38th Floor
New York, NY 10007
(929) 221-6535
dataprivacy@dss.nyc.gov

Chief Program Accountability Officer
Office of Program Accountability
151 West Broadway, 6th Floor
New York, NY 10013
(212) 274-5600
gharteys@dss.nyc.gov

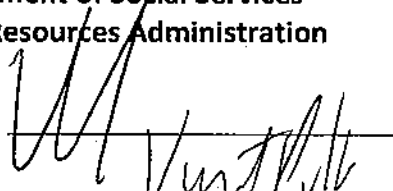
X. Cloud computing provisions

All privacy, confidentiality, security and compliance requirements set out in this Agreement shall apply to any cloud computing solution proposed for use by the HRA to accomplish any obligation under this Agreement.


Signatures

Each of the undersigned acknowledges that they have read, understand, and agree to abide by all of the terms and conditions of this MOU, and that each of them is authorized to enter into this MOU on behalf of their respective entities, with the intent to be bound thereby.

The City of New York
Department of Social Services
Human Resources Administration

Signature 
Printed Name Anthony Ventrella
Title Asst. Dir.
Date 11/18/19

State of New York
Office of Temporary and Disability
Assistance

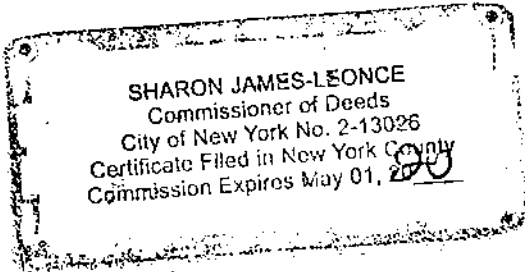
Signature 
Printed Name Krista Rock
Title General Counsel
Date 11/5/19

STATE OF NEW YORK)

: SS:

COUNTY OF NEW YORK)

On this 18th day of November 2019, before me personally came Vincent Pulio to me known and known to me to be NCCO of the DEPARTMENT OF SOCIAL SERVICES/HUMAN RESOURCES ADMINISTRATION of the CITY OF NEW YORK, the person described in and who executed the foregoing instrument, and he acknowledged to me that he executed the same for the purpose therein mentioned.



Sharon James Leonce
NOTARY PUBLIC

STATE OF New York)

:SS:

COUNTY OF Albany)

On this 5th day of November 2019, before me personally came Krista Rock to me known and known to me to be General Counsel of the OFFICE OF TEMPORARY AND DISABILITY ASISSTANCE of the STATE OF NEW YORK, the person described in and who executed the foregoing instrument, and he acknowledged to me that he executed the same for the purpose therein mentioned.

DAWN M. MAGUIRE
Notary Public, State of New York
Qualified in Albany Co., No. 01MA6211514
Commission Expires Sept. 21, 2021

Dawn M. Maguire
NOTARY PUBLIC

Appendix A
List of fields included on EBT file from OTDA to HRA 04/03/2019

| Column Name | Data Type | Description |
|-----------------------------|--------------|---|
| INPUT_ZIP_CD_ADDR | VARCHAR2(10) | Transaction location zip code |
| INPUT_ZIP_CD_EXT_ADDR | VARCHAR2(10) | Transaction location zip code -extended |
| INPUT_STATE_CD | VARCHAR2(2) | Transaction location state |
| INPUT_CITY_ADDR | VARCHAR2(40) | Transaction location city |
| INPUT_FULL_STREET_ADDR | VARCHAR2(64) | Transaction location full street address |
| INPUT_STREET_NBR_ADDR | VARCHAR2(10) | Transaction location street number |
| INPUT_APT_NBR_ADDR | VARCHAR2(7) | Transaction location apartment number |
| INPUT_STREET_NAME_ADDR | VARCHAR2(47) | Transaction location street name |
| INPUT_PO_BOX_NBR_ADDR | VARCHAR2(9) | Transaction location PO Box Number |
| INPUT_DISP_FULL_STREET_ADDR | VARCHAR2(64) | Transaction location full street address |
| INPUT_ADDR_LINE_2_ADDR | VARCHAR2(40) | Transaction location address line 2 |
| CARD_NBR | NUMBER(19) | EBT Card Number |
| CARD_ENTRY_TYPE_CD | VARCHAR2(1) | Indicates Keyed (K), Swiped (S) or Null transaction |
| TRAN_LOCAL_DT_TIME | DATE | Local terminal transaction date and time |
| TRAN_LOG_DT_TIME | DATE | EPPIC Transaction processing Date and Time (recommended to use alt_tran_log_dt_time field instead; see note below). |
| TRAN_LOG_DT_TIME_HS | NUMBER(2) | EPPIC Transaction processing Date and Time - to the hundredth of a second |
| TRAN_LOG_DT_TIME_NBR | NUMBER(20) | Integral interpretation of tran_log_dt_time |
| FNS_NBR | VARCHAR2(7) | Unique identifier assigned to retailers by USDA. Only for SNAP transactions. |
| TRAN_TYPE_CD | VARCHAR2(3) | Transaction type code. |
| CREDIT_DEBIT_IND | VARCHAR2(2) | Indicator for Debit (DB), Credit (CR), or No Value (NV) transaction |
| REPLY_CD | NUMBER(2) | Indicates transaction completed (will always be "00" for this file) |
| REVERSAL_DT | DATE | Date of the reversal. Calendar date of the reversal which should be same as the Tran Log Date |
| Reversal_Cd | Number(2) | Code indicating transaction response type |
| PRIMARY_ALT_IND | VARCHAR2(1) | Cardholder or Authorized Representative indicator (2-Vault Card Holder; 4-Auth Rep; 8-Primary Cardholder) |

Appendix A

List of fields included on EBT file from OTDA to HRA 04/03/2019

| Column Name | Data Type | Description |
|---------------------|--------------|--|
| REQUESTED_AMT | NUMBER(8,2) | Requested Amount (does not include a surcharge amount or ATM fee) |
| COMPLETED_AMT | NUMBER(8,2) | Authorized transaction amount (total completed transaction amount, includes surcharges and ATM fees) |
| ACCOUNT_BALANCE_AMT | NUMBER(8,2) | Account balance after transaction. |
| TERMINAL_ID | VARCHAR2(10) | Terminal ID of where transaction took place, as sent in by switch or assigned in EPPIC. Applies to financial transactions and balance inquiries. |
| TRACE_NBR | NUMBER(8) | Authorization number assigned to Manual Authorization Hold vouchers on 104 transaction types |
| PROGRAM_TYPE_CD | VARCHAR2(2) | Indicates program type: 01-SNAP, 02-Cash |
| CASHBACK_AMT | NUMBER(6,2) | Cashback amount. Non-blank, must contain a value of \$0.00 or actual dollar amount |
| MERCHANT_NM | VARCHAR2(15) | Transaction location Name. |
| COUNTY_CD | VARCHAR2(2) | County code of cardholder. |
| CENTER_NBR | VARCHAR2(3) | NYC Only, value sent with original benefit. If transaction spans multiple centers, uses the most recent center for the transaction. |
| CASE_NUMBER_ID | VARCHAR2(14) | Case number, including county and suffix id. If transaction spans multiple case numbers, uses the most recent case number for the transaction. |
| DISTRICT_CD | VARCHAR2(2) | 2 character county code of cardholder. |
| CASE_ID | VARCHAR2(10) | 10 character case number |
| SUFFIX_ID | NUMBER(2) | 2 character suffix id. |
| DEBIT_ACCOUNT_ID | NUMBER(12) | Internal EPPIC id. |
| SURCHARGE_CD | VARCHAR2(1) | Indicator used for surcharges on Cash transactions from the ATM owner. Must be either Y or N. |
| SURCHARGE_AMT | NUMBER(5,2) | Surcharge amount for cash transactions from the ATM owner. If Surcharge Amount greater than zero, Surcharge Indicator will be "Y". |
| ATM_FEE_CD | VARCHAR2(1) | Indicates the \$0.45 withdrawal fee is being charged to the cardholder. Fee is included in the Completed Amount. Y or N values. |
| RESTAURANT_CD | VARCHAR2(1) | N/A - always blank. |

Appendix A

List of fields included on EBT file from OTDA to HRA 04/03/2019

| Column Name | Data Type | Description |
|--------------------------|--------------|---|
| SETTLEMENT_DT | DATE | Settlement date of the transaction |
| CIN_ID | VARCHAR2(10) | Client Identification Number |
| SSN_ID | VARCHAR2(9) | SSN of cardholder |
| CBIC_CARDHOLDER_NM | VARCHAR2(28) | Cardholder Name |
| PAYEE_BIRTH_DT | DATE | Cardholder DOB |
| TRAN_ID | VARCHAR2(6) | 6 character id used in conjunction with other fields to identify primary key |
| ALT_TRAN_LOG_DT_TIME | DATE | Transaction Date and Time - This field should be used to identify date/time of transaction. |
| ALT_TRAN_LOG_DT_TIME_IND | VARCHAR2(1) | "Y" for benefit updates, "N" for all other transactions |
| CONTROL_CYCLE_NBR | NUMBER(6) | Unique number assigned to each detail transaction batch file received from vendor. All transaction records on a specific file will have this control cycle number assigned. |

Note: It is recommended to use alt_tran_log_dt_time instead of tran_log_dt_time for transaction date/time due to the manner in which the vendor posts client benefits. The tran_log_dt_time for benefit updates will display settlement date, not the date the benefit is available for use by the client. The alt_tran_log_dt_time field has been included to reflect the actual date/time of all debit and credit transactions, including when benefit updates are available to client.

Appendix B
CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT
CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

With regard to my work with _____ (Requestor)

I,

_____ am:

(INDIVIDUAL's name)

- An employee of Requestor
- A volunteer with Requestor
- A contractor of Requestor
- An employee of a contractor of Requestor
- A volunteer with a contractor of Requestor
- A subcontractor to a contractor of Requestor
- An employee of a subcontractor to Requestor
- A volunteer with a subcontractor to Requestor

and I understand that, as part of performing my duties as an employee, volunteer, contractor or subcontractor, I may have access to, see or hear "Protected Information," which, for purposes of this agreement, shall include, but not be limited to:

1. Data or information maintained in and/or obtained from OTDA and social services districts-owned applications, systems, networks and/or databases. Data or information maintained in and/or obtained from any other device, application, hardware, software, system, network and/or database created and/or maintained by a third party contractor, agent, vendor, or subcontractor which may be encompassed by this Agreement.
2. Data or information identifying an individual, particularly where such disclosure could result in an unwarranted invasion of personal privacy. Such data or information may include, but is not limited to: home addresses; telephone numbers; Social Security numbers; client identification numbers; payroll information; financial information; health information; and/or, eligibility and benefit information;
3. Computer codes or other electronic or non-electronic data or information, the disclosure of which could jeopardize the compliance stature, security or confidentiality of OTDA's information technology solutions, applications, systems, networks or data;
4. Non-final OTDA policy or deliberative data or information related to the official business of OTDA;
5. Data or information which is not otherwise required to be disclosed under the NYS Freedom of Information Law;

Appendix B
CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

6. Any other material designated by OTDA as being “Confidential,” “Personal,” “Private” or otherwise “Sensitive.”

I acknowledge and agree that all Protected Information (oral, visual or written, including both paper and electronic) which I see or to which I have access shall be treated as strictly confidential and shall not be released, copied or otherwise re-disclosed, in whole or in part, unless expressly authorized by the New York State Office of Temporary and Disability Assistance (OTDA).

I understand and agree that access to and the use of Protected Information obtained in the performance of my duties shall be limited to purposes directly connected with such duties, unless otherwise provided in writing by OTDA. When access to such information or data also results in access to Protected Information or data beyond that which is necessary for the purpose for which access was granted, I agree to access only that Protected Information needed for the purpose for which access was given.

When I no longer require the use of or access to such Protected Information, I agree that I will not access or attempt to access any Protected Information, including, but not limited to any Protected Information in State systems or other sources, to which I have been given access. I will return any and all reports, notes, memoranda, notebooks, drawings, data and other Protected Information developed, received, compiled by or delivered to me in order to carry out my functions or which may be in my possession, regardless of the source of the Protected Information. Any Protected Information not returned will be catalogued, and thereafter securely scrubbed, shredded, or otherwise disposed of in accordance with New York State EISO policies [<http://www.its.ny.gov/tables/technologypolicyindex>].

I understand that federal and State law and regulation prohibit the release or disclosure of such Protected Information, in whole or part. I acknowledge and hereby agree that I will not copy, re-disclose or otherwise share Protected Information in whole or in part in any form to anyone unless I am expressly directed to do so by my supervisor and such disclosure complies with applicable federal and State law and regulation. I further understand that if I am unsure as to what information is confidential, I will immediately, and prior to any such access, use, or re-disclosure, consult with OTDA or my supervisor.

I will safeguard, and will not disclose to unauthorized parties, any user name and/or password that may be issued to me in furtherance of my access to the Protected Information unless authorized. I understand that my access to Protected Information may be revoked at any time if my responsibilities change, or for any other reason at the discretion and direction of OTDA, or my supervisor. Further, I will not facilitate access or disclosure of Protected Information to any unauthorized person or entity, whether by knowingly providing my user name and/or password or otherwise.

I will comply with all applicable Federal and State confidentiality, record security, compliance and retention laws, regulations, policies and procedures.

I will immediately report to my supervisor any activities by any individual or entity that I have reason to believe may compromise the availability, integrity, security or privacy of the Protected

Appendix B
CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

Information. I will immediately notify OTDA and my supervisor of any request for Protected Information that does not come from an individual directly involved in the project.

I agree not to attach or load any hardware or software to or into any State or Requestor equipment unless properly authorized, in writing, to do so by OTDA. I will use only my access rights to, and will access only those systems, directories, and Protected Information authorized for my use by OTDA.

I will not use OTDA telecommunications, Internet, E-mail or other services or equipment for any illegal, disruptive, unethical or unprofessional activities, for personal gain, or for any purpose that could jeopardize the legitimate interests of the State or expose some or all Protected Information.

I agree not to knowingly take any actions that may intrude upon, disrupt or deny OTDA or Requestor services or the flow of any Protected Information.

I agree to store any Protected Information received in secure, locked containers or, where stored on a computer or other electronic media, in accordance with state and federal law and regulation, as well as OTDA's and New York State Office of Information Technology Services' (ITS) security policies that protects Protected Information from unauthorized disclosure.

I understand and agree that the terms of this Agreement shall continue even when I am no longer an OTDA or Requestor employee, contractor, subcontractor, or volunteer and that I will abide by the terms of this Agreement in perpetuity.

I understand that failure to comply with these requirements may result in disciplinary action, termination, civil action and/or criminal prosecution, as well as any other penalties provided by law.

This Agreement shall be governed by the laws of the State of New York, unless otherwise required by Federal law.

(INDIVIDUAL's Signature)

(INDIVIDUAL's Printed Name)

(Entity of which INDIVIDUAL is an employee, subcontractor or volunteer)

(Date)

Appendix B

CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

Legal and Regulatory References

This policy addresses and incorporates compliance with a variety of Federal and State statutory, regulatory and policy requirements related to confidentiality, privacy and information security, including but not limited to the following:

Public Assistance

- Fair Hearing records: 45 C.F.R. § 205.10(a)(19); 18 NYCRR 357; 18 NYCRR 358-3.7; 18 NYCRR 358-4.3; 18 NYCRR 358-5.11(b); 18 NYCRR 387.2(j)
- General rules: SSL § 136; 18 NYCRR §§ 357.1 – 357.6
- IRS and State Tax Information: 26 U.S.C. § 6103(l)(7); 26 U.S.C. § 6103(L)(8); SSL §§ 23; 136-a(2); NY Tax Law §§ 697(e)(3), 1825; *see also* IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies (2014), *available at* www.irs.gov/pub/irs-pdf/p1075.pdf
- Welfare Management System (WMS) data: SSL § 21

Medical Assistance

- General rules: 42 U.S.C. § 1396a(a)(7), *amended by* Pub. L. No. 113-67, 127 Stat. 1165 (2013); 42 C.F.R. § 431.300 et seq; SSL §§ 136, 367-b(4), 369(4); 18 NYCRR 357.1 – 357.6; 18 NYCRR 360-8; Public Health Law § 2782 (AIDS information)
- HIPAA regulations: 45 C.F.R. pt. 160; 45 C.F.R. pt. 164

Supplemental Nutrition Assistance Program (SNAP)

- General Rules: 7 U.S.C. § 2020(e)(8); 7 C.F.R. § 272.1(c); 7 C.F.R. § 278.1(q); 18 NYCRR 387.2(j); 18 NYCRR 357

Other Statutes and Policies

- Criminal Offenses involving Computers (including governmental and personal records): NY Penal Law art. 156
- Freedom of Information Law: NYS Public Officers Law, Article 6, §§ 84 – 90

Appendix B
CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

- Internet Security and Privacy Act: State Technology Law 201-208; N.Y.S. Executive Order No. 117, 9 NYCRR 5.117 (Jan. 28, 2002)
- NYS Office of Information Technology Services, Information Technology Standard, Cyber Incident Response NYS-S13-005
- NYS Office of Information Technology Services, Information Technology Policy, Information Security NYS-P03-002
- Personal Privacy Protection Law: NYS Public Officers Law, Article 6-A, §§ 91 – 99
- State Archives and Records Administration: Arts and Cultural Affairs Law 57.05 and 57.25