nrs nationwide recovery services

PO Box 8005
Cleveland, TN 37320

Exhibit A to City of Chattanooga Letter

February 7, 2025

VIA U.S. MAIL

Attn: Chief Financial Officer
City of Chattanooga
100 East 11th St.
Chattanooga, TN 37402

Re: NATIONWIDE RECOVERY SERVICES, INC. DATA SECURITY EVENT

Nationwide Recovery Services, Inc. ("NRS") is writing to supplement our July 14, 2024 notice regarding the July 11, 2024 cyber incident. We are writing to inform you that we recently determined the incident may impact the security of certain information related to individuals associated with CITY OF CHATTANOOGA. Although we have no evidence to suggest there has been identity theft or fraud related to this incident, NRS is providing this notice to make you aware of the incident and to inform you of the steps we are offering to take in response.

As you are aware, in July 2024, NRS discovered suspicious activity related to certain systems which resulted in a network outage. We immediately took steps to secure our environment and launched an investigation to determine the nature and scope of the activity. The investigation determined there was unauthorized access to the NRS network between July 5, 2024, and July 11, 2024, and that certain files and folders were copied from our systems. As a result, NRS began a review of the systems which contained these files and folders to determine what information they contained and to which NRS client the information belongs.

This review was recently completed, and we are notifying you because we determined that information related to individuals associated with CITY OF CHATTANOOGA is potentially impacted as a result of this incident. The information that may be potentially impacted likely includes name, address, social security number, date of birth, financial account information and/or medical related information, among other information provided to NRS as part of its normal course of business.

The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon becoming aware of this incident, we immediately took steps to confirm the security of our systems and to determine what information was potentially impacted. We implemented additional cybersecurity measures and reviewed existing security policies to further protect against similar incidents moving forward. We are notifying potentially impacted clients and reported this incident to federal law enforcement.

You may have certain legal duties in response to this matter, including providing notice of this incident to the individuals associated with your organization and whose information was potentially impacted, and we recommend you share this letter with legal counsel. You may also have contractual notice obligations as well. On behalf of CITY OF CHATTANOOGA, NRS is offering to provide written notice of this incident, complimentary credit monitoring, and call center services to potentially affected individuals associated with your organization. We will also provide notification of this incident to applicable U.S. state regulators, as requested.

Upon request, we will securely send you a list of individuals associated with CITY OF CHATTANOOGA that NRS identified. Subject to your written authorization, notice will be provided to these individuals by way of a letter in substantially the same form as the sample letter attached as ***Exhibit A***.

If you would like NRS to take these steps on your behalf, please provide the following information:

1. Authorization to mail notice to potentially affected individuals associated with your organization on your behalf.
2. Authorization to provide potentially affected individuals associated with your organization access to complimentary credit monitoring.
3. Complete address information for any potentially affected individuals in which you would like NRS to provide written notice to; and
4. Authorization to provide notice to U.S. state regulatory bodies, if required, and direction to which U.S. state regulatory bodies you would like notified.

NRS will not take any further action on your behalf unless written authorization to do so is provided.

Please contact us at Privacy@nrsagency.com with any questions or concerns. If you would like NRS to take any of the above actions on your organization's behalf, please provide written authorization to NRS no later than March 15, 2025.

We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Nationwide Recovery Services, Inc.

nrs nationwide recovery services

EXHIBIT A

<<First Name>> << Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

[Date]

<< Variable Data 2>>

Dear <<First Name>> << Last Name>>:

Nationwide Recovery Services, Inc. ("NRS") is writing on behalf of <<data owner name>>to inform you of an incident that may impact the security of some of your information. NRS is a debt collection agency and received your information in its normal course of business. We are providing you with information about the incident, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? In July 2024, NRS discovered suspicious activity related to certain systems which resulted in a network outage. We immediately took steps to secure our environment and launched an investigation to determine the nature and scope of the activity. The investigation determined there was unauthorized access to the NRS network between July 5, 2024, and July 11, 2024, and that certain files and folders were copied from our systems. As a result, NRS began an extensive review of these files and folders to determine what information they contained and to which NRS client the information belonged. This review was completed on or about February 3,2025.

What Information Was Involved? NRS undertook an in-depth review process to identify the individuals and NRS clients who were potentially impacted. NRS is notifying you now out of an abundance of caution because the investigation recently determined that certain information relating to you may have been within the accessed systems, including your name and <<Variable Data 1>>. Please note that we do not have any evidence of identity theft and fraud as a result of this incident.

What We Are Doing. We take this incident and the security of information in our care very seriously. Upon becoming aware of this incident, we immediately took steps to confirm the security of our systems and conduct an investigation. We also reviewed existing security policies and implemented additional measures to further protect against similar incidents moving forward. We reported this incident to law enforcement and regulators, as required by law.

In addition to providing you with notice of the event, we are also offering you immediate access to complimentary credit monitoring and identity theft protection services for <<Membership Offering Length>> months, through <Vendor>. You can find information on how to enroll in these services in the below *Steps You Can Take to Help Protect Your Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits and health insurance/medical bills, and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. Please also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information* where you may also find instructions to activate the credit monitoring and identity theft protection services we are offering.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-xxx-xxx-xxxx Monday through Friday, x:xx a.m. to x:xx p.m., <Time Zone> Time. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Nationwide Recovery Services, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

[enrollment instructions]

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact directly the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.).
2. Social Security number.
3. Date of birth.
4. Addresses for the prior two to five years.
5. Proof of current address, such as a current utility bill or telephone bill.
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov. You can also write to NRS at <mailing address>.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. You can also write to NRS at <mailing address>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [#] Rhode Island residents that may be impacted by this event.