Notice of the Sirva, Inc. Data Event

November 16, 2024

Sirva, Inc. ("Sirva") is a provider of moving and relocation services for other entities. Its family of brands include Sirva, Sirva Relocation, Sirva Move Management, Sirva Moving Services, Sirva Commercial Moving, Sirva Worldwide, BGRS, Allied International (for household goods moving) Allied Moving Services, Allied Van Lines, Allied Pickfords, northAmerican Van Lines, northAmerican International (for household goods moving), northAmerican Moving Services Alliance, Sirva Mortgage, SMARTBOX, and Global Van Lines. In addition to notices which have been previously provided directly to involved individuals and business-related customers, Sirva is providing general notice of an event that may affect the security of certain data, including data Sirva received from its individual and business-related customers. This notice provides information about the event, Sirva's response to date, and the resources available to individuals to help protect their information from possible misuse, should they feel it appropriate to do so.

What Happened? Sirva became aware of suspicious activity involving its network and immediately began an investigation. The investigation determined that certain Sirva systems were accessed by unknown actors between August 16, 2023 and October 17, 2023, and during this time certain files were copied. Sirva then undertook a thorough review of the potentially involved data to identify its contents and to whom the contents relate. The review is ongoing. Sirva began notifying the clients associated with this information and has worked with them to notify potentially impacted individuals on a rolling basis.

What Information was Involved? To date, Sirva's investigation identified that the following types of personal information could have been involved: an individual's name; address; Social Security/Insurance number; driver's license or other government identification numbers; financial account information, in limited cases with a form of an access code; tax identification information, email addresses (both business and personal), in limited cases with an access code; a form of a signature; and, other sensitive employment and hiring related information including employment IDs.

What Sirva Is Doing. Sirva takes this event and the security of information in its care very seriously. Upon becoming aware of the suspicious activity, Sirva moved immediately to investigate, assess and secure its network to ensure continuity of normal business operations for its customers, review the relevant involved files, notify potentially involved clients and associated individuals, and notify federal law enforcement and regulators, as applicable. As part of Sirva's ongoing commitment to the privacy and the security of its environment, Sirva has also reviewed and made enhancements to its existing policies and procedures.

For More Information. If you have additional questions, you may contact our dedicated assistance line toll-free at +1 (615) 863-1870 (calling from outside of the United States) and 1(866) 528-7586 (calling within the United States). This line is available 24 hours a day, 7 days a week. You may also write to Sirva, Inc. at 17W110 West 22nd Street, Oakbrook Terrace, IL 60181 or visit Sirva's website at https://www.sirva.com/.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 one-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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
1-888-298-0045	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

As a best practice, consumers should change all passwords to their personal accounts on a regular basis, use strong passwords, and refrain from using the same password for multiple accounts. Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 727-3400; and https://oag.dc.gov.

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/.

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; (919) 716-6400; 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 (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 3 Rhode Island residents that may be impacted by this event.

Steps You Can Take to Help Protect Your Information

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

You may request that creditors contact you before deciding to extend credit based on the information in your credit report by placing a "Potential Fraud Warning" on your credit file with the following credit bureaus:

TransUnion
Consumer Relations / Centre de relations au consommateur
3115 Harvester Road, Suite 201
Burlington, ON L7L 3N8 (EN) 1-800-663-9980
(FR) 1-877-713-3393
https://www.transunion.ca

Equifax Canada
National Consumer Relations
P.O. Box 190, Station Jean-Talon
Montreal, Quebec H1S 2Z2
1-800-465-7166
https://www.consumer.equifax.ca

A "Potential Fraud Warning" remains on your file for a period of six (6) years. Request to amend or remove of the Potential Fraud Warning from your file must be made in writing.

You can also learn more about identity theft and the steps you can take to protect yourself, by contacting the Canadian Anti-Fraud Centre (https://www.antifraudcentre-centreantifraude.ca/).

As an added precaution and based on the information involved, we recommend that you:

- stay cautious when answering calls from unfamiliar numbers, or talking to or following instructions from someone you do not know;
- never open attachments or click on links in emails or social media messages (such as messages on Facebook) from unknown senders; and
- inform yourself of email, telephone and text-based scams.

Generally, we also recommend not sharing your personal information with anyone online, via email or on social media unless you are absolutely certain about with whom you are sharing it.