

Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street Suite 3900
Chicago Illinois 60601
T (312) 985-5900
F (312) 985-5999

September 27, 2021

Via Electronic Mail

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

To Whom It May Concern:

We represent OneSource Virtual, Inc. (“OSV”) with respect to a data security incident described in more detail below. OSV is providing this notice at the request of its customers, who are listed on Exhibit A. OSV is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident

On August 10, 2021, OSV discovered that an employee inadvertently e-mailed a password protected spreadsheet containing confidential benefits information for other customers to two employees of an OSV customer, which occurred on August 1, 2021. Both recipients were contacted and confirmed that the report was deleted, and that they did not misuse, forward, download, share, print, or otherwise copy the report. The recipients work frequently with benefits information and are familiar with the importance of protecting personal information.

The data file contained individuals’ names, ID Numbers, COBRA Assistance for Eligible Individual subsidy status, Social Security numbers, qualifying event dates, first date of coverage, last day of coverage, event type or reason, qualified beneficiary status in the COBRA system (active or terminated), and the plan type the qualified beneficiary was offered on COBRA (dental, medical or vision, for example).

2. Number of residents affected

The number of residents that may have been affected and were notified of the incident are listed on Exhibit A. A notification letter was sent to the potentially affected individuals on September 27, 2021 via regular mail (a copy of the form notification letter is enclosed as Exhibit B).

3. Steps taken in response to the incident

September 27, 2021

Page 2

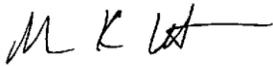
Additionally, in response to this incident, OSV has re-trained the personnel involved on the importance of handling sensitive personal information and OSV's learning and development group is creating a module that will be rolled out to the entire company about these types of issues. Although OSV believes misuse of the data is highly unlikely, residents notified of the incident were offered 12 months of credit monitoring and identity protection services through IDX. Notice of this incident was not provided to law enforcement as it did not involve criminal activity.

4. Contact information

OSV takes the security of the information in its control seriously and is committed to ensuring the information in its control is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Very truly yours,

CLARK HILL

A handwritten signature in black ink, appearing to read 'M K Ventrone', with a long horizontal flourish extending to the right.

Melissa K. Ventrone
Partner

Enclosures

EXHIBIT A –New Hampshire Resident

	1
	1 Residents

onesource
VIRTUAL
 P.O. Box 989728
 West Sacramento, CA 95798 9728

To Enroll, Please Call: 1-833-513-2612 Or Visit: https://app.idx.us/account-creation/protect Enrollment Code: <<Enrollment>>
--

<<FirstName>> <<LastName>>
 <<Address1>>
 <<Address2>>
 <<City>>, <<State>> <<Zip>>

September 27, 2021

NOTICE OF DATA SECURITY INCIDENT

Dear <<FirstName>> <<LastName>>,

OneSource Virtual, Inc. (“OSV”) recently experienced a data security incident that may have impacted your personal information. OSV assists enterprises, including <<Variable Text 1>> in optimizing its human resources and finance software solutions. OSV received your information as part of the provision of services to <<Variable Text 1>>. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. While we believe there is no risk that any of your information will be misused, we wanted to provide you with details regarding this incident, and resources we are making available to help you.

WHAT HAPPENED?

On August 10, 2021, OSV discovered that an employee inadvertently e-mailed a password protected spreadsheet containing confidential benefits information for other customers to two employees of an OSV customer. Both recipients were contacted and confirmed that the report was deleted, and that they did not misuse, forward, download, share, print, or otherwise copy the report. The recipients work frequently with benefits information and are familiar with the importance of protecting personal information. Because of this, we do not believe there is any risk your information will be misused, but wanted to let you know about this incident out an abundance of caution.

WHAT INFORMATION WAS INVOLVED?

The information contained in the report includes your name, ID Number, COBRA Assistance for Eligible Individual subsidy status, Social Security number, qualifying event date, first date of coverage, last day of coverage, event type or reason, qualified beneficiary status in the COBRA system (active or terminated), and the plan type the qualified beneficiary was offered on COBRA (dental, medical or vision, for example).

WHAT WE ARE DOING

Although we do not believe there is any risk that your information will be misused, we are offering identity theft protection services through IDX, the data breach and recovery services expert, at no charge to you. IDX identity protection services include: <<12 / 24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. You can enroll in free identity protection services by calling 1-833-513-2612 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is December 27, 2021.

Additionally, in response to this incident, we have re-trained the personnel involved on the importance of handling sensitive personal information and are currently in the process of reviewing our policies and procedures involving the secure transfer of sensitive personal information.

WHAT YOU CAN DO

While we believe there is no risk that your information will be misused, it is always a good idea to remain vigilant for incidents of identity theft or fraud, and to review your bank account and other financial statements as well as your credit reports for suspicious activity. We also encourage you to contact IDX with any questions and to take full advantage of the IDX service offering. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

If you have any questions or concerns, please call 1-833-513-2612 Monday through Friday from 8 am - 8 pm Central Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

A handwritten signature in black ink that reads "Erin B. Clark". The signature is written in a cursive, flowing style.

Erin Clark
General Counsel
OneSource Virtual, Inc.

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

- 1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-833-513-2612 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

Experian Fraud Reporting and
Credit Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_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.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.