



April 18, 2023

Richard Bortnick
312.881.3334 (direct)
richard.bortnick@wilsonelser.com

Via Email

Attorney General Brian Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Cybersecurity Incident Involving Communication Services d/b/a Interprettek

Dear Attorney General Frosh:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Communication Services d/b/a Interprettek (“Interpretek”), a sign language interpretation service provider located at 75 Highpower Road, Rochester, NY 14623, with respect to a recent cybersecurity incident that was first discovered by Interpretek on January 20, 2022 (hereinafter, the “Incident”). Interpretek takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of residents being notified, and the steps that Interpretek has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On or about January 20, 2022, Interpretek became aware of a potential business e-mail compromise (the “Incident”). Upon discovering the Incident, Interpretek immediately engaged a third-party professional cybersecurity forensic team to conduct a thorough investigation into its entire e-mail tenant and determine the nature and scope of the Incident. On April 7, 2022, the forensic investigation determined that an unknown party had gained unauthorized access to one (1) Interpretek employee e-mail user account.



55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

Although Interprettek is unaware of any fraudulent misuse of information, it is possible that individuals' full name, addresses; financial account numbers; driver's license/state ID numbers; username in combination with passwords; health insurance information; personal health information; and/or social security numbers may have been exposed as a result of this unauthorized activity.

As of this writing, Interprettek has not received any reports of related identity theft since the date of the incident (January 20, 2022 to present).

2. Number of Maryland residents affected.

A total of 2 Maryland residents have been potentially affected by this incident. Notification letters to these individuals were mailed on April 17, 2023, by first class mail. A sample copy of the notification letters are included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Interpretek is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, Interprettek moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, Interprettek engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, Interprettek is continuing to enhance security measures and providing cyber security training for its staff; implementing Endpoint Detection and Response (EDR) software throughout the environment; encrypting local machines and emails; migrating data to Azure; implementing email spam and DNS filtering; implementing Dark Web monitoring; implementing firewall management; and implementing Multi Factor Authentication on email and Office 365. This investigation and response included confirming the security of Interprettek's systems, reviewing the contents of the relevant files for sensitive information, and notifying business partners associated with that sensitive information.

Although Interprettek is not aware of any actual or attempted misuse of the affected personal information, Interprettek offered (12) months of complimentary credit monitoring and identity theft restoration services through Epiq to all individuals to help protect their identity. Additionally, Interprettek provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

Interpretek remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at richard.bortnick@wilsonelser.com or 619-881-3334.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Richard Bortnick

EXHIBIT A



Communication Services, Inc. d/b/a Interpretek

Return Mail Processing Center

P.O. Box 6336

Portland, OR 97228-6336

VIA FIRST-CLASS MAIL

<<Mail ID>>

<<Name 1>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

To Enroll, Please Visit:

www.equifax.com/activate

Membership Number:

<<Activation Code>>

<<Mail Date>>

Notice of Data Incident

Dear <<Name 1>>:

Communication Services, Inc. d/b/a Interpretek ("Interpretek") recently experienced a data security incident which may have affected your personal information. We take the protection and proper use of your information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to safeguard your information.

What Happened

On or about January 20, 2022, Interpretek became aware of a potential incident affecting its e-mail environment (the "Incident"), which may have resulted in the unauthorized access to individuals' personal information. We have since worked diligently to determine what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of your personal information that were exposed may have included, and potentially were not limited to your: name, address, <<data elements>>. Please note that there is no evidence at this time that any of your personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity experts to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to strengthen our security posture to prevent a similar event from occurring again in the future.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (1-Bureau Credit Watch Gold) for twelve (12) months provided by Equifax, one of the three nationwide credit reporting companies.

You can sign up for the credit monitoring service anytime between now and **June 31, 2023**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with Equifax, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain twelve (12) months of unlimited access to your Equifax credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

What You Can Do

To enroll in this service, go to the Equifax website at www.equifax.com/activate and in the space referenced as “Enter Activation Code”, enter the following Activation Code <<Activation Code>> and follow the steps to receive your credit monitoring service. Please see more information regarding the enrollment process at the end of this letter.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. The FTC also provides information on-line at www.ftc.gov/idtheft.

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following page, which contains important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 888-996-4592 Monday – Friday, 9:00 am to 9:00 pm Eastern Time.

Sincerely,

Interpretek

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
equifax.com/personal/credit-report-services/
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.