**From:** Moore, Desiree F.
**To:** DOJ: Attorney General
**Subject:** Notice of Security Incident
**Date:** Wednesday, May 5, 2021 6:20:46 PM
**Attachments:** Final SEIU 775 Benefits Group Ad r2prf.pdf



To whom it may concern:

Please be advised that we are legal counsel for SEIU 775 Benefits Group. We write regarding a recent data security incident. Specifically, on or about April 4, 2021, internal SEIU 775 Benefits Group IT personnel detected certain anomalies in SEIU 775 Benefits Group's data systems, including what appeared to be the potential deletion of information. Upon a thorough investigation led by third-party cybersecurity and forensic consultants, SEIU 775 Benefits Group has determined that unknown individuals appear to have gained access to SEIU 775 Benefits Group systems. In doing so, the unknown individuals deleted certain information, including certain personally identifiable information ("PII"). To date, there is no evidence that the unknown individuals downloaded or exfiltrated or otherwise accessed this or other information, and SEIU 775 Benefits Group has seen no use or misuse of the information.

Fifteen (15) New Hampshire residents were potentially affected by the incident.

Attached is a sample notification letter that will be mailed to New Hampshire residents on or about May 10, 2021.

If you have any questions or require any additional information, please do not hesitate to contact me directly. Thank you.

Best regards,

Desiree

**Desiree Moore**
Partner
K&L Gates LLP
desiree.moore@klgates.com

70 W. Madison St.
Suite 3100
Chicago, IL 60602
Phone: +1 312 781 6028

www.klgates.com

19271_DCPR_email_graphic1

SEIU 775
BENEFITS GROUP

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

**Notice of Data Security Incident**

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

**What happened?**

On or about April 4, 2021, internal SEIU 775 Benefits Group IT personnel detected certain anomalies in SEIU 775 Benefits Group's data systems, including what appeared to be the potential deletion of information. Upon a thorough investigation led by third-party cybersecurity and forensic consultants, SEIU 775 Benefits Group has determined that unknown individuals appear to have gained access to SEIU 775 Benefits Group systems. In doing so, the unknown individuals deleted certain information, including certain personally identifiable information ("PII") and Protected Health Information ("PHI") protected under the Health Insurance Portability and Accountability Act ("HIPAA"). To date, there is no evidence that the unknown individuals downloaded or exfiltrated or otherwise accessed this or other information, and SEIU 775 Benefits Group has seen no use or misuse of the information.

**What information was involved?**

The information that may have been compromised could include your demographic information, such as your name, address, and social security number, as well as, potentially, health plan eligibility or enrollment information.

**What we are doing.**

Upon detecting the incident, SEIU 775 Benefits Group immediately took action to secure the affected systems and contain the incident. SEIU 775 Benefits Group then notified federal law enforcement authorities and other stakeholders, and, as noted above, retained leading third-party cybersecurity and forensic consultants to investigate the nature and scope of the incident. SEIU 775 Benefits Group also engaged legal counsel and is in the process of notifying any other relevant authorities as may be required. In the aftermath of the incident and on an ongoing basis, SEIU 775 Benefits Group internal teams continue to work diligently with third-party cybersecurity consultants to further fortify SEIU 775 Benefits Group systems.

Additionally, to help relieve concerns and restore confidence following this incident, SEIU 775 Benefits Group has secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response. Their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **August 13, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing services available to you is included with this letter.

**What you can do.**

In addition to activating the identity monitoring services, please review the enclosed “Additional Resources” section included with this letter. This section describes additional steps you can take to help protect yourself, 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, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:00 p.m. Pacific Time, excluding major U.S. holidays. Please have your membership number ready. Protecting your information is paramount to us and we hope that the services we are offering to you demonstrate our commitment in this regard. Thank you for all you do to care for others. It’s our honor to serve you with health, training, and secure retirement benefits.

Sincerely,

Abby Solomon
Chief Executive Officer
SEIU 775 Benefits Group

## ADDITIONAL RESOURCES

**Contact information for the three nationwide credit reporting agencies:**

**Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
**Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
**TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

**Free Credit Report.** It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Fraud Alerts.** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Security Freeze.** You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, 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 5 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, and display your name, current mailing address, and the date of issue.

**Federal Trade Commission and State Attorneys General Offices.** If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

**For 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/.

**For Connecticut residents:** You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

**For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

**Reporting of identity theft and obtaining a police report.**

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

### Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

### Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

### $1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.