

Jason M. Schwent
T (312) 985-5939
F +13125177573
Email:jschwent@clarkhill.com

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

October 29, 2024

VIA ELECTRONIC MAIL

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown:

We represent Foley Material Handling Co. (“Foley”) with respect to a data security incident involving personal information described below. Foley takes the security of the information in its control seriously and is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident from occurring in the future.

1. Nature of security incident.

On May 14, 2024, Foley discovered suspicious activity on its systems, immediately implemented its incident response protocols, and began an internal investigation. Foley also engaged cybersecurity and data forensic specialists to assist with determining what occurred and whether any data was compromised. On September 12, 2024, the investigation determined that personal information belonging to customers of Foley was impacted. Types of information that were present on Foley’s system for those customers and clients include: names, addresses, dates of birth, driver’s license numbers, and Social Security numbers.

2. Number of residents affected.

Two (2) Maryland residents were notified of the incident. A notification letter was sent to the potentially affected individuals on October 25, 2024 (a copy of the form notification letter is enclosed as Exhibit A).

3. Steps taken in response to the incident.

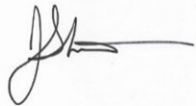
Since the incident, Foley has hardened their web application firewalls, completed additional third-party penetration testing, added additional full-time resources for security specific code reviews and anomalous system user/activity behavior, and enhanced other existing security controls.. Additionally, potentially affected individuals was/were offered 12 months of credit monitoring and identity protection services through TransUnion at no cost.

4. Contact Information

Foley takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read 'JS', followed by a long horizontal line.

Jason M. Schwent

JMS:mm

<<Company name>>

c/o Cyberscout

<<Return Address1>> <<Return Address2>>

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

11327 VIRGINIA CRANE DRIVE
POST OFFICE BOX 289
ASHLAND, VIRGINIA 23005



TELEPHONE (804) 798-1343
FAX (804) 798-7843
www.foleymaterialhandling.com

<<First Name>> <<Last Name>>

<<Address1>> <<Address2>>

<<City>>, <<State>> <<PostalCode+4>>

<<Date>>

<< Custom Field 1 >>

DEAR <<FIRST NAME>> <<LAST NAME>>,

Foley Material Handling Company, Inc. ("Foley") is writing to let you know about a data security incident that may have impacted some of your information. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened?

In May 2024, we identified suspicious activity from an unauthorized user on our systems. Foley immediately implemented its incident response protocols, began an investigation, and engaged independent computer forensic experts to assist with an investigation of what happened. The investigation determined that the unauthorized user gained access to documents on the Foley system. A vendor was hired to review the potentially impacted documents to identify any personal information that was present at the time of the unauthorized access. From the review, it appears that your personal information may have been contained in the documents. Foley has no evidence that your information has been misused, however, we wanted to make you aware of this incident out of an abundance of caution.

What Information Was Involved?

It appears that your <<Exposed Data Elements>> may have been affected.

What We Are Doing:

We have taken steps to prevent this kind of event in the future, such as changing passwords for email accounts and reinforcing multi-factor authentication is implemented on email accounts.

In addition, although there has been no evidence your information was misused, we are offering identity theft protection services by Cyberscout, a TransUnion company for <<Service length>>. With this protection, Cyberscout will help you resolve issues if your identity is compromised.

What You Can Do:

You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary credit monitoring services being offered to you by logging on to <https://bfs.cyberscout.com/activate> and following the provided instructions. When prompted, please provide the following unique code: <<Unique Code>>. To receive the monitoring services, please enroll within 90 days from the date of this letter. The enrollment requires an internet connection and email account and may not be available to minors. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

This letter also provides other precautionary measures you can take to protect your information. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information:

If you have questions, please call 1-800-405-6108, Monday through Friday from 8:00 a.m to 8:00 p.m. Eastern Time, excluding holidays. Protecting your information is important to us, and we sincerely apologize for any concern this incident may cause you.

Sincerely,

Richard A. Foley/CEO

Foley Material Handling Company, Inc.

Recommended Steps to help Protect your Information

1. Website and Enrollment.

Foley Material Handling Company, Inc, is providing you with information about steps that you can take to help protect your personal information and is offering you complimentary identity protection services. These services provide you with alerts when changes occur to your credit file for <<Service length>> from the date of enrollment. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, Foley is providing you with proactive fraud assistance to help with any questions that you might have or if you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. The complimentary credit monitoring services being offered to you by logging on to <https://bfs.cyberscout.com/activate> and following the provided instructions.

2. 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.

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.

3. 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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

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

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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.

4. 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.

5. 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.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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/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.

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. A total of [XX] Rhode Island residents were notified of 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.