



Richard W. Goldberg
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Richard.Goldberg@lewisbrisbois.com
Direct: 215.977.4060

File No. TBD

March 10, 2022

VIA EMAIL

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

Re: **Notice of Data Security Incident**

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Hanchett Paper Company d/b/a Shorr Packaging Corporation ("Shorr") in connection with a data security incident that may have affected the information of certain Maryland residents. The purpose of this letter is to notify you of the incident in accordance with Maryland Code Ann. Com. Law §§ 14-3501.

1. NATURE OF THE SECURITY INCIDENT

Shorr is an industrial packaging distributor of paper packaging and shipping products. It is headquartered in Aurora, Illinois, with over 500 employees nationwide.

On January 31, 2022, Shorr experienced a data security incident that affected its network. Shorr immediately launched an investigation and engaged cybersecurity experts to help determine what happened and what information may have been accessed. On February 8, 2022, the investigation determined that an unknown actor gained access to its network and may have obtained data from the Shorr network without authorization.

Shorr undertook a review of the information that could have potentially been accessed as a result of the incident. Shorr determined that information related to its employees and their beneficiaries, including the personal information of five (5) Maryland residents, was potentially impacted. The information potentially accessed without authorization may have included the individual's first and last name, social security number, date of birth, and financial account information. To date, Shorr has

no evidence that any potentially impacted information has been misused in conjunction with this incident.

2. NUMBER OF MARYLAND RESIDENTS AFFECTED

Shorr notified the five (5) Maryland residents of this data security incident via first class U.S. mail on March 10, 2022. A sample copy of the notification letter sent to the affected individuals is attached.

3. STEPS TAKEN RELATING TO THE INCIDENT

Shorr implemented additional security features to reduce the risk of a similar incident occurring in the future. Shorr also reported this incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to attempt to hold the perpetrators of this incident accountable, if possible.

While Shorr has no indication that the information has been misused, it nonetheless is providing individuals with information about steps that they can take to help protect their personal information. As a further precaution, Shorr is also offering the Maryland consumers one (1) year of complimentary credit and identity monitoring services through IDX. This product helps detect possible misuse of personal information and provides consumers whose information may have been accessed without authorization with identity protection support.

4. CONTACT INFORMATION

Shorr is committed to protecting the security of the personal information in their possession. Please feel free to contact me at Richard.Goldberg@lewisbrisbois.com or by phone at 215-977-4060 if you have any further questions.

Sincerely,



Richard W. Goldberg of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

RWG
Enclosure: Sample Consumer Notification Letter



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-903-3648
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: XXXXXXXXX

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>

March 10, 2022

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a recent data security incident experienced by Hanchett Paper Company d/b/a Shorr Packaging Corporation ("Shorr"), that may have involved your personal information. Shorr takes the privacy and security of all personal information very seriously. This letter contains information about the recent incident, steps you can take to help protect your personal information, and resources that Shorr is making available to assist you.

What Happened:

On January 31, 2022, Shorr experienced unauthorized access to our network and promptly initiated a comprehensive plan including isolating and powering down all systems. We immediately engaged with industry-leading cybersecurity experts to assist with the response and investigation. Although we have no reason to believe that any personal information has been misused at this time, out of an abundance of caution, Shorr is providing credit and identity monitoring for its employees, former employees, and their families at no cost to help reduce concerns that you may have about the incident.

What Information Was Involved:

The information types of personal information may have been involved: your name, Social Security number, date of birth, and bank account information.

What We Are Doing

In addition to the steps described above, Shorr is diligently working with cybersecurity experts to further strengthen the security of the network. We have teams working around the clock, and we will continue to do so until we can ensure a safe and secure return to operations. In addition, we have reported the incident to the law enforcement and will assist in their investigation to locate the people who did this.

To help relieve concerns and restore confidence following this incident, Shorr has secured the services of IDX to provide credit monitoring for adults and identity monitoring for family members who are minors, at no cost to you for, <<12/24>> months. IDX is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include credit monitoring, identity monitoring; \$1 million in identity theft expense reimbursement insurance; and fraud prevention and resolution support.

To receive credits services, you must be over the age of 18, 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. Additional information describing your IDX services is included with this letter.

Visit <https://app.idx.us/account-creation/protect> to activate and take advantage of your identity monitoring services.

You have until June 10, 2022 to activate your identity monitoring services.

Enrollment Code: Can be found above

To enroll in identity protection services, please call 1-833-903-3648 or log on to <https://app.idx.us/account-creation/protect> and use the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 a.m. and 9 p.m. Eastern Time. Please note the deadline to enroll is June 10, 2022.

What You Can Do:

Shorr encourages you to activate the credit and identity monitoring services we are making available through IDX. Also, please review the enclosed "Additional Resources" section included with this letter. It describes additional steps you can take to help protect yourself, including recommendations regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We remind you to stay vigilant and watch out for signs of fraud and identity theft in your account statements and credit reports.

For More Information:

If you have questions, please call 1-833-903-3648, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and privacy.

Sincerely,



Robert Onorato,
Chief Executive Officer
Hanchett Paper Company / Shorr Packaging Corporation

(Enclosure)

ADDITIONAL RESOURCES

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
www.ftc.gov/idtheft
1-877-438-4338

Illinois Attorney General
100 West Randolph Street
Chicago, Illinois 60601
illinois.attorneygeneral.gov
1-877-844-5461

Ohio Attorney General
30 E. Broad Street, 14th Floor
Columbus, Ohio 43215
www.ohioattorneygeneral.gov
1-800-282-0515

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
www.iowaattorneygeneral.gov
1-888-777-4590

Indiana Attorney General
302 West Washington Street, 5th floor
Indianapolis, Indiana 46204
in.gov/attorneygeneral
1-800-457-8283

Georgia Attorney General
2 Martin Luther King Jr. Drive, Ste. 365
Atlanta, Georgia 30334-9077
law.georgia.gov
1-404-651-8600

New York Attorney General
28 Liberty Street
New York, NY 10005
ag.ny.gov/consumer-frauds-bureau
1-800-771-7755

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Maryland Attorney General
200 St. Paul Place
Baltimore, Maryland 21202
oag.state.md.us
1-888-743-0023

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.