CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

MEGHAN FARALLY
MFarally@c-wlaw.com

January 16, 2025

Via E-Mail (IDTheft@oag.state.md.us)
Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Edw. C. Levy Co. ("Levy") located at 9300 Dix Ave, Dearborn, MI 48120. We write to provide notification of a cyber security incident. By providing this notice, Levy does not waive any rights or defenses under Maryland state law, including the data breach notification statute.

On November 1, 2023, Levy discovered that it was victimized by a sophisticated ransomware attack. Upon discovery, Levy immediately began working with its I.T. team and third-party forensic specialists to investigate the full nature and scope of the incident. Levy also reported this incident to federal law enforcement. While the investigation was still ongoing, it was determined that certain Levy files containing information related to Levy employees may have been subject to unauthorized access as part of the attack. In an abundance of caution, Levy provided notice to potentially impacted employees on December 27, 2023. There were no Maryland residents present in the initial employee population.

As the investigation continued, Levy learned that an employee email account was subject to unauthorized access as part of the incident. Upon discovery, Levy performed a comprehensive review of the contents of the email account and provided notice to individuals whose personal information was contained therein accordingly. This set of notifications was sent on February 12, 2024. There were no Maryland residents present in the notice population related to the email account.

Further investigation revealed a larger data set of Levy files that may have been subject to unauthorized access. As a result, Levy, with the assistance of third-party specialists, undertook a comprehensive and time-intensive process to identify the information that may have been contained within the potentially impacted files, and to whom that information belonged. Levy then undertook a time-consuming, manual review of its internal records in order to locate address information for those potentially impacted.

While the comprehensive review process remains ongoing, on December 19, 2024, Levy determined that information related to 5 Maryland residents may have been subject to unauthorized access. The information believed to be at risk may include a first and last name, in combination with a Social Security number.

On January 16, 2025, Levy provided written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland state law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to individuals is substantially similar to the letter attached hereto as **"Exhibit A."**

As the investigation continues, if additional Maryland residents are discovered to be potentially impacted, we will notify this office accordingly.

Please contact me should you have any questions.

Very truly yours,

Meghan Farally, Esq.
CIPRIANI & WERNER, P.C.

EXHIBIT A

Edw. C. Levy Co.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

January 16, 2025

P 000010102G0500

Dear [redacted]

We are writing to inform you of a cyber security incident experienced by Edw. C. Levy Co. that may have involved your information as described below. While we have no evidence of attempted or actual misuse of any information, we are providing you with information about the incident, our response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened: On November 1, 2023, we were victimized by a sophisticated ransomware attack that impacted our network. Upon discovery, we immediately began working with our I.T. team and third-party forensic specialists to investigate the full nature and scope of the incident. We also reported this incident to federal law enforcement. Through the investigation, we learned that certain files, kept in the normal course of business, may have been subject to unauthorized access during the incident. Upon discovery, with the assistance of third-party specialists, we immediately began a comprehensive and time-intensive review of the impacted files to determine the type of information contained therein and to whom that information related. While this comprehensive process remains ongoing, we are notifying those individuals known to date whose information may have been subject to unauthorized access.

What Information Was Involved: The information believed to be at risk may include your first and last name, in combination with your [redacted]

What We Are Doing: Upon discovery, we immediately engaged third-party forensic specialists to investigate this matter. Out of an abundance of caution, we have arranged for you to activate, at no cost to you, Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score for twelve months provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

What You Can Do: We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can enroll to receive the complimentary credit monitoring services we are making available to you. You can also review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center agents at 1-833-799-4246 from 8 a.m. to 8 p.m. Eastern Time, Monday through Friday, excluding major holidays.

We take the privacy and security of the information in our care seriously, and sincerely regret any worry or inconvenience this incident may cause you and your family.

Sincerely,

Kristen A. Locklear
VP Human Resources

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. 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.

ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion	Experian	Equifax
1-800-680-7289 www.transunion.com	1-888-397-3742 www.experian.com	1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	**Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013	**Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	**Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. Edw. C. Levy Co. may be contacted at 9300 Dix Ave, Dearborn, MI 48120.

For 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 bureaus 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 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. We encourage you to 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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-722 6 or 1-919-716-6000; and www.ncdoj.gov.