

October 5, 2022

Sent Via Email Only

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

Re: *Notice of Data Security Breach – Erdman and Hockfield, LLP*

Dear Attorney General Frosh:

I am writing on behalf of our client, Erdman and Hockfield, LLP, a North Carolina law firm located at 2300 East Seventh Street, Suite 100, Charlotte, NC 28204-3313 (the “Firm”). I write to notify you, pursuant to Md. Comm. Code § 14-3504, of a data security incident involving two (2) Maryland residents.

Discovery and Nature of Breach

In late August 2021, the Firm fell victim to the Lockbit 2.0 ransomware variation. The perpetrators of the attack demanded that the Firm pay a ransom to gain access to the files that had been encrypted on its network servers. The Firm immediately contacted its third-party information technology (“IT”) management provider to assess the nature and scope of the incident.

At the time of the ransomware attack, the Firm used various virus protection and anti-malware programs, including but not limited to, Microsoft Windows Defender Antivirus, Vipre Email Security, Webroot, and BitDefender Ransomware. Staff was trained to use the software and not to open emails from unknown sources. The Firm backed up its servers with a Backup Assist program at the end of each workday.

The Firm’s Response

Fortunately, at the time of the incident, the Firm had sufficient backups to recover virtually all of the encrypted data. The Firm initiated the recovery process and was able to continue servicing its clients with little-to-no disruption. The Firm did not pay the ransom or otherwise acknowledge to the perpetrators that it had received the ransomware notice. The perpetrators have not contacted the Firm since the initial ransom event.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

After recovering from backups, the Firm sought assistance from industry professionals, including from counsel submitting this notice and from a qualified cyber forensics investigator, to further investigate the incident. With assistance from these professionals, the Firm conducted an extensive programmatic and manual review of all potentially impacted data. Much of this data was unstructured and required, which pushed completion to July 5, 2022. This review revealed that Maryland residents who were not clients of the firm were affected by the ransomware attack. The Firm contacted their client representative associated with the file in which the Maryland residents' information appeared to let that person know of the incident and obtain updated addresses to provide notice.

Notice to Affected Persons

The Firm will mail formal notice of this incident to the affected Maryland residents in substantially the same form as Attachment 1 to this letter. This notice will be mailed on October 6, 2022.

The Firm previously mailed notice to affected clients in North Carolina, where it provides legal services, on July 14, 2022.

If you have any other questions or need additional information, please let me know.

Sincerely yours,



S. Wilson Quick

Attachment

1 – Sample Consumer Notification Letter

ERDMAN AND HOCKFIELD, LLP

ATTORNEYS AT LAW
2300 EAST SEVENTH STREET, SUITE 100
CHARLOTTE, NORTH CAROLINA 28204-3313

DAVID W. ERDMAN
STEVEN A. HOCKFIELD

704-333-7800
Fax 704-343-2886

October 6, 2022

Re: Notice of Data Security Breach

Dear correspondent,

This notice is to inform you of a data security incident that may impact the privacy of some of your information. Although we are currently unaware of any misuse of your information, we take this incident seriously, and write to provide you with information about what happened, steps we have taken in response, and steps you can take to help protect your privacy.

What Happened? In late August 2021, we were impacted by a ransomware attack. The perpetrators of the attack demanded that we pay a ransom to gain access to our files that they encrypted on our network servers. We immediately contacted our information technology management team to access the nature and scope of the incident. Upon realizing that we had sufficient backups to recover virtually all of the encrypted data, we initiated the recovery process and were able to continue servicing our clients with little-to-no disruption. We chose not to pay the ransom or otherwise acknowledge to the perpetrators that we had even received the ransomware notice. The perpetrators have not contacted us since the initial ransom event.

What Information Was Involved? As lawyers, we receive a wide variety of personal information from our clients and about those with whom our clients interact. With the help of third-party forensic and legal experts, we undertook a thorough, time-intensive review of the contents of the files that were encrypted. Following that review we determined that some element of your "Personally Identifiable Information" (Tax ID Number, Social Security Number, account number, etc.) was potentially accessible to the unauthorized person.

What We Are Doing. For nearly three decades, data security has been a key element of this firm's DNA. We have always taken steps to protect the information we receive. Our practice is to shred hard-copy documents that include personal information. We review and regularly update our data security practices and procedures, including through the use of virus protection software and by installing relevant software patches and updates.

After this incident occurred, and with help from our information technology management team, we confirmed that there was no malicious software present on or suspicious activity in our servers. We redoubled our efforts at sharing best practices in information security with our attorneys and staff. We continue to review and update firm email and document retention policies to help reduce the risk of this type of incident in the future.

What You Can Do. You are encouraged to remain vigilant against identity theft and fraud by regularly reviewing account statements and monitoring credit reports for suspicious activity. Please review the enclosed "Further Information to Help Protect Your Privacy" to learn about additional steps you can take to help protect your information, including by placing a free fraud alert on your credit report, obtaining a free copy of your credit report, and accessing additional resources.

For More Information. We understand that you may have questions. If so, please contact us at the telephone number above Monday through Friday from 9:00 AM to 5:00 PM Eastern Time to speak with us about this incident. We value your relationship with us and apologize for any inconvenience or concern this incident causes you. Thank you.

Erdman & Hockfield LLP
By: David Erdman & Steve Hockfield

FURTHER INFORMATION TO HELP PROTECT YOUR PRIVACY

Place a fraud alert on your credit report. You have the option of placing a fraud alert on your credit report. A fraud alert is free of charge and easy to place. You may contact toll-free any one of the three major credit bureaus listed below. As soon as one bureau confirms your report, the others are simultaneously notified on your behalf.

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

Obtain a copy of your free credit report. You may also obtain a free copy of your credit report from each of the three major credit reporting bureaus once every 12 months by visiting www.annualcreditreport.com, calling toll-free (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, Georgia 30348. It is recommended that you monitor your free credit reports for incidents of fraud and identity theft.

Review your account statements and monitor credit reports. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing your financial account statements and monitoring your free credit reports for unauthorized access. Doing so can help you spot problems and address them quickly.

Notify law enforcement of any suspicious activity. You should also notify the appropriate law enforcement authorities, your state attorney general, and/or the U.S. Federal Trade Commission (FTC) of any suspected identity theft.

Additional resources to protect against identity theft. You can find additional information to help protect yourself from identity theft, including information about fraud alerts and credit report security freezes, by contacting one of the three major credit bureaus listed above, or by visiting the FTC's website at www.ftc.gov/idtheft, by calling 1-877-ID-THEFT (1-877-438-4338), or by writing to the Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580.

Maryland residents may wish to review information provided by the Office of the Attorney General of Maryland, Consumer Protection Division at www.oag.state.md.us/Consumer, by calling 1-888-743-0023, or writing to 200 St. Paul Place, Baltimore, MD 21202.