BakerHostetler

Baker&Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

October 19, 2016

VIA EMAIL (SECURITYBREACH@ATG.WA.GOV)
AND FIRST CLASS MAIL

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

Our client, Eastwood Company (Eastwood), is deeply committed to protecting the security and confidentiality of its customers' information. On July 22, 2016, Eastwood learned that malicious software code may have been inserted into its e-commerce website. Eastwood immediately removed the malicious software, began an investigation and hired a third-party cybersecurity firm to assist.

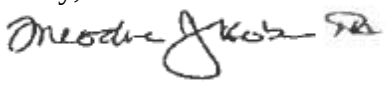
Findings from the investigation show that if a customer placed an order on Eastwood's website from May 29, 2016 to July 22, 2016, information associated with the order being placed, including the customer's name, address, phone number, email address, payment card number, expiration date and security code (CVV) may have been obtained by an unauthorized third-party. Additionally, if a customer placed an order as a new Eastwood customer during this timeframe, the password to their account may have also been exposed.

Eastwood provided written notification via U.S. Mail on October 19, 2016, to 633 Washington residents in accordance with Wash. Rev. Code § 19.255.010 in substantially the same form as the document enclosed herewith. Notice is being provided in the most expedient time possible and without unreasonable delay, upon completion of the PCI Forensic Investigation that was required by the payment card brands and that was subject to the process of obtaining images of the servers maintained by a third-party. Eastwood has also established a dedicated call center to answer any questions that individuals may have regarding the incident.

To help prevent this from happening again, Eastwood has remediated its e-commerce website and continues to work to strengthen the security of the website.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Theodore J. Kobus III
Partner

Enclosure

DO THE JOB RIGHT.

October 19, 2016

[redacted]

Dear [redacted]

The Eastwood Company (Eastwood) values the relationship we have with our customers and understands the importance of protecting customer information. We are writing to inform you about an incident that may involve some of your information.

On July 22, 2016, Eastwood learned that malicious software code may have been inserted into its e-commerce website. We immediately removed the malicious software, began an investigation and hired a third-party cybersecurity firm to assist us. Findings from the investigation show that if a customer placed an order on our website from May 29, 2016 to July 22, 2016, information associated with the order being placed, including the customer's name, address, phone number, email address, payment card number, expiration date and security code (CVV) may have been obtained by an unauthorized third-party. If you placed an order as a new Eastwood customer during this timeframe, your password to your account may have also been exposed. We are notifying you because you placed an order on www.eastwood.com using a payment card(s) ending in [redacted] during the relevant time period.

We encourage you to remain vigilant to the possibility of fraud and identity theft by reviewing your financial statements for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution because the major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported. You should also review the additional information on the following page on ways to protect yourself. If you placed an order as a new customer during the affected timeframe, we recommend changing the password to your Eastwood account.

We apologize for any inconvenience or concern this may have caused. To help prevent this from happening again, we have remediated our e-commerce website and continue to work to strengthen the security of the website.

If you have questions, please call 1-866-331-5685, Monday through Friday, from 9 a.m. to 7 p.m. EST (Closed on U.S. observed holidays).

Sincerely,

Brian Huck
Chief Operating Officer

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
Experian, PO Box 4500, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

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 state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW
Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

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 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with 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.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

If you are a resident of Maryland, North Carolina, or Rhode Island, you may contact and obtain information from your state attorney general at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland (410) 576-6300 (for calls originating outside Maryland)
North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400
Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400