

STATE OF NH
DEPT OF JUSTICE
2020 NOV 16 AM 9:14

BakerHostetler

Baker & Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

Jennifer E. Costa
direct dial: 713.646.1344
jcosta@bakerlaw.com

November 13, 2020

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, E.W. Wylie Corporation (“E.W. Wylie”), to notify you of a security incident involving one New Hampshire resident.

On September 25, 2020, E.W. Wylie discovered unusual activity within its network. E.W. Wylie immediately took steps to secure its network and investigate the activity. As part of the investigation, an independent computer forensic firm was engaged to help determine what happened and whether any personal information had been accessed without authorization. On October 9, 2020, E.W. Wylie determined that an unauthorized individual acquired certain documents from its network. The documents involved contained the personal information of one New Hampshire resident including their name and Social Security number.

On November 13, 2020, E.W. Wylie mailed a notification letter to the New Hampshire resident in substantially the same form as the enclosed letter via U.S. First-Class mail in accordance with N.H. Rev. Stat. Ann. § 359-C:20. E.W. Wylie is offering a complimentary, one-year membership to credit monitoring and identity protection services to all letter recipients. E.W. Wylie has also established a dedicated, toll-free call center where individuals may obtain more information regarding the incident. Furthermore, E.W. Wylie has alerted the three major consumer reporting agencies.

To help prevent a similar incident from occurring in the future, E.W. Wylie has implemented additional measures and changes to enhance the security of its network.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Dallas Denver Houston
Los Angeles New York Orlando Philadelphia San Francisco Seattle Washington, DC Wilmington

Attorney General Gordon MacDonald
November 13, 2020
Page 2

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

Sincerely,

A handwritten signature in black ink, consisting of several overlapping loops and a long horizontal stroke extending to the right.

Jennifer E. Costa
Counsel

Encl.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

E.W. Wylie Corporation (“E.W. Wylie”) is committed to protecting the confidentiality and security of its employees’ personal information. I am writing to inform you of an incident that involved some of your personal information. This notice explains the incident, measures that have been taken, and some steps you can take in response.

What Happened?

On September 25, 2020, we discovered unusual activity within our network. We immediately took steps to secure our network and investigate the activity. As part of the investigation, an independent computer forensic firm was engaged to help determine what happened and whether any personal information had been accessed without authorization. On October 9, 2020, we determined that an unauthorized individual acquired certain documents from our network.

What Information was Involved?

Based upon our review of the information involved, on October 13, 2020, we determined the information involved includes your <<b2b_text_1(ImpactedData)>>.

What We Are Doing.

As soon as we discovered the incident, we took the steps discussed above. In addition, in an effort to prevent similar incidents from occurring in the future, we have implemented additional measures to enhance the security of our network. We are also providing you with information about steps you can take to protect your personal information and have alerted the three major consumer reporting agencies. Furthermore, we have arranged for you to receive a complimentary twelve-month membership to identity monitoring services through Kroll. Kroll is a global leader in risk mitigation and response, and its team has extensive experience assisting people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, a \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

What You Can Do.

You can follow the recommendations on the following page to protect your personal information. In addition, we encourage you to activate the free identity monitoring services that are being offered to you.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **February 11, 2021** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

For More Information:

We regret that this incident occurred and apologize for any inconvenience. If you have any questions about the incident, please contact our dedicated helpline at [1-800-800-8000](tel:1-800-800-8000), Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time. Please have your Membership Number ready to provide to the call center agent.

Sincerely,

A handwritten signature in black ink, appearing to read "Scott Hoppe", with a long horizontal flourish extending to the right.

Scott Hoppe
President & CEO | E.W. Wylie Corporation

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

ADDITIONAL STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free 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 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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. 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. 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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general 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 one year. 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.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland: E.W. Wylie is located at 2500 43rd Street North, Fargo, ND 58102, and can be reached at 800-437-4132. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us.

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov.

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.