

# 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

August 5, 2021

### VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella  
Office of the Attorney General  
33 Capitol Street  
Concord, NH03301

*Re: Incident Notification*

Dear Attorney General Formella:

We are writing on behalf of our client, Atlantic Coast Dismantling, LLC (“ACD”), to notify you of a security incident.

ACD recently completed an investigation that involved suspicious activity within its email environment. Upon learning of the unauthorized access on January 20, 2021, ACD immediately took steps in an effort to ensure its email tenant was secure. In addition, a cybersecurity firm was engaged, and a thorough investigation was conducted. The investigation determined that there was unauthorized access to two ACD employee email accounts.

ACD conducted a careful review of the email accounts to identify individuals whose information may have been accessed. On June 23, 2021, ACD identified seventeen New Hampshire residents whose personal information was potentially involved, including the residents’ names and one or more of the following: (1) Social Security number; (2) driver’s license number; or (3) financial account information, including bank name, account number, and routing number.

Beginning today, August 5, 2021, ACD is mailing a notification letter via United States Postal Service First-Class mail to the seventeen residents in accordance with N.H. Rev. Stat. Ann. § 359-C:20. ACD is offering a complimentary, one-year membership of identity monitoring services provided by Kroll to individuals whose Social Security numbers and/or driver’s license numbers were involved. ACD also established a dedicated phone number where the individuals may obtain more information regarding the incident.

Attorney General John Formella  
August 5, 2021  
Page 2

To reduce the risk of a similar incident occurring in the future, ACD has implemented additional measures to enhance the security of its email environment.

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

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

Enclosures



<<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>>:

Atlantic Coast Dismantling, LLC is committed to protecting the confidentiality and security of the personal information we maintain. I am writing to inform you of an incident that potentially involved some of your personal information. This notice explains the incident, measures we have taken, and some steps you may consider taking in response.

### **What Happened?**

We recently concluded an investigation into an incident involving unauthorized access to two employee email accounts. Upon discovering the incident, we immediately took steps to ensure our email environment was secure, a cybersecurity firm was engaged, and a thorough investigation was conducted. The investigation found that there was unauthorized access to two employee email accounts. The investigation was unable to determine whether any emails or attachments were actually viewed by an unauthorized individual during that time. In an abundance of caution, we reviewed the contents of the two email accounts to identify the individuals whose personal information they contained. We then located each person's contact information for purposes of providing notice. We completed that process on June 23, 2021.

### **What Information Was Involved?**

Based upon the investigation, we determined that the personal information involved includes your <<b2b\_text\_1(ImpactedData)>>.

### **What We Are Doing.**

We take the security of your data very seriously. In an effort to prevent a similar incident from occurring in the future, we have implemented additional measures to enhance the security of our email environment.

As a precaution, we arranged for you to receive a complimentary one-year membership of identity monitoring services through Kroll. Kroll is a global leader in risk mitigation and response, and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. To enroll in the identity monitoring services being offered at no cost to you, please follow the instructions below:

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

You have until October 26, 2021 to activate your identity monitoring services.

Membership Number: <<Membership Number s\_n>>

For more information on identity theft prevention and additional steps you may consider taking in response, please see the information provided with this letter.

### **What You Can Do.**

While we have no indication that your personal information has been misused as a result of this incident, we wanted to notify you and assure you that we take this incident very seriously. We also encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institution immediately.

**For More Information:**

We regret that this occurred and apologize for any inconvenience. If you have any questions about the incident, please feel free to contact our dedicated helpline at [1-800-877-7777](tel:1-800-877-7777), Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

Sincerely,



Ralph W. Marchant  
CEO | Atlantic Coast Dismantling, LLC



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

### Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll 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.

### 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.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and 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 STEPS YOU CAN TAKE

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](http://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](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://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](http://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](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://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.

ACD's mailing address is 63 Salem Turnpike, Saugus, MA 01906, and its phone number is (617) 884-7700.

#### **Additional information for residents of the following states:**

**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>.

**Rhode Island:** This incident involves [three Rhode Island residents](#). Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, [www.riag.ri.gov](http://www.riag.ri.gov).