



A business advisory and advocacy law firm®

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: (410) 456-2741
Cell: (410) 917-5189
E-mail: spollock@mcdonaldhopkins.com

April 27, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: R.J. Smith Construction - Security Breach Notification

Dear Mr. Brown:

We are writing on behalf of our client, R.J. Smith Construction (located at 1711 Reymet Road N., Chesterfield, VA 23237), to notify you of a data security incident involving six (6) Maryland residents.¹

Nature

On or about March 15, 2022, R.J. Smith Construction discovered suspicious activity in one of its employee email accounts involving an attempt to gain control of its financial account. After discovering the incident, R.J. Smith Construction acted quickly to secure the email account and investigate the incident.

At the conclusion of the investigation, R.J. Smith Construction determined that an unauthorized actor likely gained access to the employee email account, and as a result, likely obtained protection personal information. R.J. Smith Construction conducted a comprehensive review to determine the types of protected information contained within account and to identify individuals potentially impacted by the incident. R.J. Smith Construction recently determined that the incident potentially involved six (6) Maryland residents. Further, on or about April 19, 2023, R.J. Smith Construction located the most recent contact information for these individuals.

The personal information obtained potentially included first and last name, date of birth, driver's license number, passport number, military or government identification or federal identification number, license plate and VIN number, Social Security number, routing and/or financial account number, credit or debit card information, username and password, medical information, and health insurance information.

¹ By providing this notice, R. J. Smith Construction does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Notice and R.J. Smith Construction's Response to the Event

On April 28, 2023, R.J. Smith Construction will mail a written notification to the potentially affected Maryland residents, pursuant to Md. Code Com. Law § 14-3504, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, R.J. Smith Construction is providing the potentially impacted individual the following:

- Free access to credit monitoring services for one year through TransUnion;
- Guidance on ways to protect against identity theft and fraud;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Further, R.J. Smith Construction provided notice to the applicable government regulators, officials, and other state Attorneys General (as necessary).

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 456-2741 or email me at spollock@mcdonaldhopkins.com.

Sincerely Yours,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock".

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

RJ Smith Construction
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB07147 1-1



1711 Reymet Road N.
Chesterfield, VA 23237



April 28, 2023

Re: Notice of Data Security Incident

Dear [REDACTED]

At RJ Smith Construction, we value transparency and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your protected personal information, what we did in response, and steps you can take to protect yourself against possible misuse of the information.

What Happened

On or about March 15, 2022, we discovered suspicious activity in one of our employee email accounts involving an attempt to gain control of our financial account. At that time, we acted quickly to secure the email account and conduct an investigation into the incident.

At the conclusion of our preliminary investigation, we determined that an unauthorized actor likely gained access to the employee email account, and as a result, likely obtained protected personal information. With this understanding, we began a comprehensive review of the affected email account. On April 4, 2023, we concluded our review and determined that the impacted data may have contained some of your protected personal information.

Based on our investigation, and the nature of the fraudulent activity, we believe this was solely an attempt to obtain funds from our financial account (which was not successful). We have no evidence that your information has been used for identity theft or financial fraud. However, we wanted to notify you of the incident, out of an abundance of caution, and provide you information on how to best protect your identity.

What Information Was Involved

The types of information included your [REDACTED]

To reiterate, we have no evidence indicating that any information has been used for identity theft or financial fraud.

What We Are Doing

The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, we are considering additional cybersecurity protocols and safeguards, as needed, to help minimize the likelihood of this type of incident occurring again.

What You Can Do

{10897160: }

As stated above, while we have no evidence indicating that your information has been used for identity theft or fraud, we strongly recommend that you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record, as well as law enforcement. In addition, please see “***OTHER IMPORTANT INFORMATION***” on the following pages for guidance on how to best protect your identity.

Finally, we are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] 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.

For More Information

We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about what happened beyond what is covered in this letter. If you have additional questions, please call the dedicated toll-free helpline set up specifically for this purpose at [REDACTED] Monday through Friday, 8:00 a.m. to 8:00 p.m. (ET, excluding major U.S. holidays).

Sincerely,

Jody Pierson
Vice President
RJ Smith Construction
1711 Reymet Road N.
Chesterfield, VA 23237

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting <http://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, GA 30348. You can access the request form at <https://www.annualcreditreport.com/index.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. In addition, in some states, the agency cannot charge you to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below).

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

Consider Placing a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>. For more information, please visit [IdentityTheft.gov](https://www.consumer.ftc.gov/topics/identity-theft) or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at <https://www.consumer.ftc.gov/>.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 2001, <https://oag.dc.gov/consumer-protection>, Telephone: 1-202-727-3400.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392