



Jason M. Schwent
T (312) 985-5939
Email: jschwent@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

November 9, 2022

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Attorney General Frosh:

We represent Snavely Insurance and Financial Services (“Snavely”) with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. Snavely is a full-service property and casualty insurance agency and financial service agency located in St. Louis, Missouri. Snavely is committed to answering any questions you may have about the data security incident, the response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On May 10, 2022, Snavely identified suspicious activity associated with its email environment. Snavely immediately began an internal investigation and hired independent computer forensic experts to help with determining what occurred and the scope of individuals that may have been impacted. The investigation concluded on or around June 30, 2022 at which point Snavely determined that there was unauthorized access to one (1) email account. The investigation, unfortunately, could not determine exactly what materials within that email account may have been viewed, or accessed so Snavely conducted a search of the contents of the affected email. On October 10, 2022, Snavely determined that personally identifiable information was present within the account. Snavely provided notice to all individuals whose information was in the email account at the time of the unauthorized access. Information stored in the account at the time of the unauthorized accessed was name with some combination of the following elements: Social Security number, driver’s license number, financial account number, username and password for financial account, payment card information with access code, medical information, username and password for non-financial account, and health insurance policy number.

2. Number of Maryland residents affected.

One (1) resident was notified of the incident. A notification letter was sent to the potentially affected individual on November 9, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

3. Steps taken in response to the incident.

Snavely took steps to address this incident and prevent similar incidents in the future. Since the incident, Snavely enabled multi-factor authentication and changed passwords. Additionally, affected individuals were offered twelve (12) months of credit monitoring and identity protection services through Cyberscout.

4. Contact information.

Snavely takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read 'JS', with a long horizontal line extending to the right.

Jason Schwent
Senior Attorney

cc: Sunaina Ramesh

Snavely Insurance and Financial Services, LLC

<<Return Address>>

<<City>>, <<State>> <<ZIP>>



<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<ZIP>>

<DATE>

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>,

Snavely Insurance and Financial Services, LLC (“Snavely”) experienced a data security incident that may have impacted your personal information. Snavely is full-service property and casualty insurance agency and financial service agency.

We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened?

On May 10, 2022, Snavely identified suspicious activity associated with its email environment. We immediately implemented our incident response protocols, took steps to secure the email environment, and engaged independent computer forensic experts to assist with an investigation. While the investigation determined that an unauthorized actor gained access to one (1) email account on May 10, 2022, that investigation could not determine what materials may have been actually viewed or accessed by that unauthorized actor. To determine what information was found in the affected email account, we conducted a thorough investigation of the contents of that account. On October 10, 2022, we learned that your information was present within the account. Even though your information was found in the affected email account we have no evidence that your information was viewed, removed, misused, or accessed in any way by the threat actor. We are providing you with notice about this incident out of an abundance of caution.

What Information Was Involved?

From our review, it appears that your name, <<variable text data elements>> may have been affected.

What We Are Doing:

We want to assure you that we are taking steps to minimize the risk of this happening in the future. Since the incident, we have changed passwords and enabled multi-factor authentication. In addition, while we are not aware of any misuse of your information, we have arranged for you to receive credit monitoring and identity protection services at no cost to you, as a precautionary measure.

* Services marked with an “*” require 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.

What You Can Do:

We encourage you to remain vigilant against incidents of identity theft by reviewing bank account and other financial statements. We have secured the services of Cyberscout to provide Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score* services at no charge. These services provide you with alerts for twelve 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to <https://www.xxxx.com> and follow the instructions provided. When prompted please provide the following unique code to receive services: <CODE HERE> In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your information. We also encourage you to vigilantly monitor financial statements and credit reports and immediately report any suspicious activity.

For More Information:

If you have questions, please call 1-800-405-6108 Monday through Friday from 8:00 am to 8:00 pm Eastern Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,



Owner
Snavely Insurance and Financial Services, LLC

* Services marked with an "*" require 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.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have 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.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

* Services marked with an "*" require 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 California residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For District of Columbia residents: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

For Rhode Island residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There are <<xx>> Rhode Island residents impacted by this incident.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

* Services marked with an “*” require 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.