orrick

Orrick, Herrington & Sutcliffe LLP
701 Fifth Avenue
Suite 5600
Seattle, WA 98104-7097

+1 206 839 4300

orrick.com

Aravind Swaminathan

E aswaminathan@orrick.com
D +1 206 839 4340
F +1 206 839 4301

September 8, 2022

By Email

Idtheft@oag.state.md.us

RE: Notice of Cybersecurity Incident Relating to Maryland Residents

Dear Attorney General:

We are contacting you about a recent cybersecurity incident at one of Snap's vendors, Elevate. Elevate was retained to assist Snap with contract and document analysis and migration. In June 2022, Elevate informed Snap that an unauthorized party gained access to some of Elevate's computer systems in March 2022, and that some Snap contracts and documents may have been downloaded at that time. In July 2022, Elevate informed Snap that these contracts and documents were posted on the unauthorized party's website for a short time between May 2022 and June 2022 and then were taken down. At that time, however, Elevate did not identify the particular files that were affected. On August 5, 2022, Elevate provided to Snap its final understanding of the affected files.

When Snap learned of this incident, it immediately began an investigation to determine what happened, what data was affected, and to whom it belonged. This included seeking information from Elevate and engaging a third-party data analysis firm to review affected files to identify personal information.

On August 12, 2022, Snap determined that personal information for 2 Maryland residents was affected. The affected information differs by individual and can include name, address, phone number, employee ID, Social Security number, government ID number, and health information. Snap began notifying these individuals on September 8, 2022. Snap is offering each of these individuals two-years of free credit monitoring and protection services from Kroll.

The Elevate incident did not impact or compromise any Snap systems. Snap is terminating its relationship with Elevate and re-examining its relationship with other third parties that provide services to Snap. In addition to investigating the incident and analyzing affected data, Snap has confirmed that the affected data is no longer posted to the unauthorized party's website. As part of its ongoing security operations, Snap is also reviewing its security and privacy policies and procedures. Elevate has also reported this incident to law enforcement.

A copy of the individual notice is attached to this letter. If your office requires any further information in this matter, please contact me at 206-839-4340 or aswaminathan@orrick.com.

Sincerely,

Aravind Swaminathan
Partner
Orrick, Herrington, & Sutcliffe, LLP

Snap Inc.

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

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

Notice of Data Breach

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

We are contacting you about a recent cybersecurity breach at one of Snap's vendors, Elevate, that may impact your personal information. As you know, Snap greatly values the privacy and security of your personal information, and we regret that this incident has occurred. This notice provides information on what happened and what we are doing, as well as how you can obtain credit monitoring and identity restoration services at no cost to you.

What Happened: Elevate was retained to assist Snap with contract and document analysis and migration. In June 2022, Elevate informed Snap that an unauthorized party gained access to some of Elevate's computer systems in March 2022, and that some Snap contracts and documents may have been downloaded at that time. The Elevate incident did not impact or compromise any Snap systems. In July 2022, Elevate informed us that these contracts and documents were posted on the unauthorized party's website for a short time between May 2022 and June 2022 and then were taken down.

When we learned of this incident, we immediately began a thorough investigation to determine what happened, what data was affected, and to whom it belonged. This included seeking information from Elevate and engaging a third-party data analysis firm to review affected files to identify personal information.

What Information Was Involved: On August 12, 2022, Snap determined that your personal information may have been in the affected files, including your <<b2b_text_1 ("name, address, employee ID," and data elements)>><<b2b_text_2 (data elements cont.)>>. This information was provided to Snap in connection with your employment, potential employment, contractor engagement, beneficiary status, or business transaction with Snap.

What Are We Doing: Snap is terminating its relationship with Elevate and re-examining its relationship with other third parties that provide services to Snap. In addition to investigating the incident and analyzing affected data, Snap has confirmed that the affected data is no longer posted to the unauthorized party's website. As part of our ongoing security operations, Snap is also reviewing its security and privacy policies and procedures. Elevate has also reported this incident to law enforcement.

Snap is committed to safeguarding confidential and sensitive information. We have secured for you two-years of free identity monitoring services from Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people in these situations. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. **Instructions on how to activate this service are attached to this notice**.

What You Can Do: In addition to activating in the identity monitoring services being offered to you at no charge, we encourage you to take the following precautions:

- It is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police. Additional information about how to protect your identity is contained in Appendix A.

For More Information: We regret this incident has occurred and your personal information has been impacted. If you have questions about the incident, If you have questions about the incident, please call (855) 516-3886, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your Membership Number ready.

Sincerely,

Kevin van 't Klooster
Data Protection Officer

HOW TO ACTIVATE FREE IDENTITY MONITORING

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

> Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
>
> You have until **<<b2b_text_6 (date)>>** to activate your identity monitoring services.
>
> Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also 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 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.

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.

Appendix A – Information for U.S. Residents

ADDITIONAL INFORMATION

To protect against possible fraud, identity theft or other financial loss, you should always remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you can contact your local law enforcement agency, your state's attorney general, or the Federal Trade Commission. Please know that contacting us will not expedite any remediation of suspicious activity.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free at +1 (877) 726-1014.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You may contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

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.

A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax: Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374 +1 (888) 766-0008 www.equifax.com	Experian: Credit Fraud Center P.O. Box 9554 Allen, TX 75013 +1 (888) 397-3742 www.experian.com	TransUnion: TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000 +1 (800) 680-7289 www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

California Residents: Visit the California Office of Privacy Protection (https://oag.ca.gov/privacy) for additional information on protection against identity theft.

Connecticut Residents: The Attorney General can be contacted by emailing attorney.general@ct.gov or visiting portal.ct.gov/AG.

District of Columbia Residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov, and www.oag.dc.gov.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov. You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

Kentucky Residents: The Attorney General can be contacted at Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: +1 (502) 696-5300.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

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

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: The Attorney General can be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6400; or www.ncdoj.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9332 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400; or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.