

November 3, 2023

BY EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

To Whom It May Concern:

On behalf of Selling Simplified Group, Inc. (“SSG”), this letter provides notice of a cybersecurity incident involving Maryland residents. SSG is a wholly-owned subsidiary of IDG Communications, Inc. d/b/a Foundry (“IDG”). SSG is a B2B marketing company headquartered in Boston, Massachusetts.

On July 20, 2023, SSG detected suspicious activity on our computer network that resulted in a disruption of certain of our systems. SSG immediately began investigating, contacted law enforcement, and engaged a forensic firm to assess, mitigate, and restore these systems.

Our investigation has determined that an unauthorized third party compromised certain user accounts and gained unauthorized remote access to our network as early as May 10, 2023. After gaining access to our network, the unauthorized third party was then able to escalate privileges, move laterally in the network, and take certain data from the network.

With the assistance of our third-party experts, we have deployed additional security measures to further strengthen the security of our network. In addition to an SSG-wide password reset, we blocked the IP addresses and domains associated with the incident, fine-tuned our email and web filtering, further enhanced our network monitoring and use of multi-factor authentication, implemented a tiered privileged account model, and enhanced our default domain policy. We have also conducted dark web monitoring and have not identified any evidence of fraud or misuse at this time.

Upon gaining access to the affected data, SSG began working to identify all affected personal information. SSG subsequently determined that the personal information associated with three Maryland residents was affected by this incident. SSG has determined that the categories of affected data included: name, Social Security number, date of birth, driver’s license information, passport information, signature, address, email address, phone number, human resources information, compensation information, tax information, photograph or video of individuals, and nationality or citizenship information.

SSG began sending individuals formal notice on October 10, 2023 via U.S. mail and has now sent formal notice to all individuals. A sample notification letter is enclosed as Exhibit A. As stated in the enclosed sample notice, SSG is providing all U.S. individuals with 24 months of free identity theft and credit monitoring services through Kroll and a dedicated call center has been established to answer individuals' questions.

SSG takes the protection of personal information seriously and is committed to answering any questions that you may have. Please do not hesitate to contact me at 508-935-4076 or Renuka_Drummond@idg.com.

Respectfully yours,

/s/ Renuka Drummond

Renuka Drummond
General Counsel
Selling Simplified Group

Enclosures
Exhibit A

Exhibit A



[Date]

[Name]

[Address]

[City, State Zip]

Notice of Data Breach

Dear [First Name],

We at the Selling Simplified Group (“SSG”) are writing to let you know about a recent cybersecurity incident that involved your personal data. Although we have no indication that your personal data was being specifically targeted, we regret that this has happened, as keeping data safe and secure is very important to us.

Who we are

SSG is a business to business marketing-as-a-service platform that helps businesses connect with other businesses that might be interested in their products or services. We hold your personal data in connection with the employment or prospective employment of individuals at SSG.

What Happened?

On 20 July 2023, we detected that an unauthorised third party gained access to our IT system and downloaded a copy of certain company files. Those files contained your personal data. The personal data that was affected includes your [insert personal data types here]. There is no indication though that the unauthorised third party was trying to misuse your personal data and we have identified no evidence of onward data leakage after detecting the above-mentioned unauthorised access.

What We Are Doing

After becoming aware of the incident, we promptly took robust steps to address the issue and began a thorough forensic investigation, with the assistance of leading outside cybersecurity experts, to ensure the incident was contained. To help prevent future incidents, we have taken measures to harden our security systems and have deployed enhanced monitoring.

We have retained Kroll, a global leader in risk mitigation and response, to provide you with two years of complimentary credit monitoring and identity theft protection services.

Your identity monitoring services include two years of complimentary Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. Please follow the steps below to take advantage of these services.

- Visit <https://enroll.krollmonitoring.com/redeem> to activate and take advantage of your identity monitoring services.
- Provide your Activation Code: <Enter Activation Code> and your Verification ID: <Enter Verification ID>
- You will have until [Insert Date 2023] to activate your identity monitoring services.

What You Can Do

We encourage you to contact Kroll and take advantage of the credit monitoring and identity theft protection services that we are offering to you free of charge. In addition, you should remain vigilant for incidents of fraud, identity theft, and errors by regularly reviewing your account statements for any unauthorized activity and monitoring free credit reports over the next twelve to twenty-four months, if available in your jurisdiction.

Notwithstanding the fact that we have seen no evidence that the unauthorised third party has tried to misuse your personal data, we recommend that you remain vigilant for suspicious emails. If you receive a suspicious email, you may want to:

- confirm that the sender of the email is someone you know by looking at the email address it came from;
- hover over links in the email before clicking on them to ensure they are taking you to the sites you expect them to; and
- do not open attachments other than those you are expecting to receive.

For More Information

We take our responsibility to protect your personal information extremely seriously. If you have any questions, please contact us at [insert Kroll call center contact information].

Sincerely,

Kumaran Ramanathan

President

Steps You Can Take to Protect Your Information

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax 1-800-525-6285 P.O. Box 740241 Atlanta, GA 30374-0241 https://www.equifax.com/personal	Experian 1-888-397-3742 P.O. Box 2104 Allen, TX 75013-0949 https://www.experian.com	TransUnion Corp 1-800-888-4213 P.O. Box 2000 Chester, PA 19016 https://www.transunion.com
--	---	---

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file

a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For Colorado and Illinois residents, information may be obtained from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For Massachusetts residents, consumers have the right to obtain a police report regarding this incident. Consumers that are victim of identity theft also have the right to file a police report and obtain a copy of it.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

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