

Holland & Knight

31 West 52nd Street | New York, NY 10019 | T 212.513.3200 | F 212.385.9010
Holland & Knight LLP | www.hkllaw.com

Mark H. Francis
+1 212-513-3572
Mark.Francis@hkllaw.com

April 26, 2021

VIA E-MAIL TO DOJ-CPB@DOJ.NH.GOV

Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street, Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notice of Security Incident

To Whom it May Concern:

I am writing on behalf of Astoria Company LLC, a Delaware limited liability company located at 6387 Camp Bowie Blvd, Ste B #631, Fort Worth TX 76126 (“Astoria”), to inform you that notice is being sent to one (1) New Hampshire resident regarding a recently discovered cyber-attack in which certain of their personal information may have been obtained without authorization.

I. Nature of the Security Incident.

On January 5, 2021, an unknown criminal actor perpetrated a cyber-attack against Astoria and gained unauthorized access to an Astoria system. That system did not have any personal information on it but it enabled the actor to access a second Astoria system on January 18, 2021 that had a database of individuals’ personal information. Between January 19 and January 29, the actor and an associate attempted on a few occasions to access personal information in the database. Astoria became aware of the intrusion on Feb 8, 2021 and took immediate steps to secure its systems and conduct an internal forensic investigation to determine what information was accessed during the intrusion.

Over the course of its investigation, Astoria found that the unknown actor took screenshots of personal information concerning approximately 70 individuals. Forensic evidence shows that attempts to access and download larger sets of personal information failed. Astoria was made aware of allegations that large sets of personal information obtained from Astoria were released on the internet, but Astoria investigated those claims and found that the posted information is not associated with Astoria—these claims are possibly part of attempted extortion effort against Astoria. Additional technical details about the cyber-attack are currently posted at <https://astoriacompany.com/cyber-update/> and Astoria’s investigation is ongoing.

II. Type of Information Compromised.

The information in the screenshots included first and last name, mailing address, email address, phone number, date of birth, social security number, driver’s license number and state, and in some instances employment information.

III. Number of Residents Affected and Notified.

One (1) New Hampshire resident has been identified as potentially affected by the incident. Notice to this resident is being sent via first class mail on or about April 27, 2021. Notification was not delayed due to a law enforcement investigation.

IV. Steps Taken to Address the Incident.

Astoria takes its responsibility to protect personal information seriously.

Astoria arranged to have Experian help protect the potentially-affected individuals from identity theft. Specifically, Astoria has made available to these individuals, free of charge, 24 months of active credit monitoring and, if needed, identity theft assistance and insurance. Please see the enclosed copy of the template notification letter for additional details.

Astoria has also provided an explanation of additional steps that potentially-affected individuals may consider taking, free of charge, to further protect themselves, including checking credit reports, utilizing fraud alert services and placing a security freeze on credit reports, as further explained in the enclosed copy of the notification letter.

Astoria is providing the individuals with a toll-free telephone number that they may call with questions about the incident, as further explained in the enclosed copy of the notification letter.

As noted above, Astoria's investigation is ongoing. Astoria remediated the issues giving rise to the attack, but it is also implementing additional safeguards to enhance the security of its systems and personal information it maintains. The incident has been reported to the FBI.

Please contact me if you have any questions.

Sincerely yours,



Mark H. Francis
Holland & Knight LLP

Cc (via email):

Scott Thompson
CEO, Astoria Company LLC
6387 Camp Bowie Blvd Ste B #631
Fort Worth TX 76126
scott@astoriacompany.com

Eric S. Crusius
Holland & Knight LLP
1650 Tysons Boulevard, Suite 1700
Tysons, VA 22102
Eric.Crusius@hklaw.com

Enclosure



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

April 27, 2021

G4134-L01-0000001 T00001 P001 *****AUTO**MIXED AADC 159



SAMPLE A. SAMPLE - L01 GENERAL
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789



RE: Important Security Notification

Dear Sample A. Sample:

Astoria Company (“**Astoria**”) recently investigated a cyber-attack and found that a third party may have obtained personal information about you. We are therefore providing notice to you of this event.

Who is Astoria? Astoria Company operates a lead exchange, connecting consumers with the products and services they seek in near-real-time across multiple industries. As a result, we maintain contact details and other personal information about individuals even if they have not had direct relationships with us.

Who was affected by this incident? During the cyber-attack, an unknown actor obtained the personal information of approximately 70 individuals. The information included first and last name, mailing address, email address, phone number, date of birth, social security number, driver’s license number and state, and in some instances employment information.

What happened? On January 5, 2021, an unknown criminal actor perpetrated a cyber-attack against Astoria and gained unauthorized access to an Astoria system. That system did not have any personal information on it but it enabled the actor to access a second Astoria system on January 18, 2021 that had a database of individuals’ personal information. Between January 19 and January 29, the actor and an associate attempted on a few occasions to access personal information in the database. Astoria became aware of the intrusion on Feb 8, 2021 and took immediate steps to secure its systems and conduct an internal forensic investigation to determine what information was accessed during the intrusion.

The investigation found that the unknown actor took screenshots of personal information concerning 74 individuals. Forensic evidence shows that attempts to access and download larger sets of personal information failed. Astoria was made aware of allegations that large sets of personal information obtained from Astoria were released on the internet, but Astoria investigated those claims and found that the posted information is not associated with Astoria—these claims are possibly part of attempted extortion effort against Astoria. Additional technical details about the cyber-attack are currently posted at <https://astoriacompany.com/cyber-update/>.



What are we doing to protect your information? Astoria is implementing additional security measures to enhance the continued security of information in its care, and the incident has been reported to the FBI.

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorksSM, including both identity detection services and assistance in the event of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: July 31, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-888-994-0277 by **July 31, 2021**. Be prepared to provide engagement number **B012228** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 2 YEAR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **1-888-994-0277**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). Identity Restoration support is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Additional resources for protect your personal information. (1) *Getting a credit report.* Under U.S. law, individuals over the age of 18 are entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the credit bureaus directly to request a free copy of their credit report.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

(2) *Placing a fraud alert.* If you believe you are at risk of identity theft, you can have the credit bureaus place a “fraud alert” on their credit file that alerts creditors to take additional steps prior to granting credit in your name. Note, however, that this may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms the fraud alert, the others are notified to place fraud alerts as well. To place a fraud alert or inquire about your credit report, here is their contact information:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
800-680-7289
www.transunion.com

(3) *Placing a security freeze.* You can also place a “security freeze” on your credit reports. This prohibits a credit reporting agency from releasing information from your credit report without your authorization. Please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests they make for new loans, credit mortgages, employment, housing, or other services. You cannot be charged to place or lift a security freeze on your credit report. A security freeze needs to be separately requested with each of the credit bureaus, and you may need to supply certain personal information in order to confirm your identify when making the request. To find out more about security freezes, you can contact the credit reporting agencies using the information below:

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

(4) *Learning more about identify theft.* You can learn more about identity theft, fraud alerts, and steps you can take to protect yourself by contacting the Federal Trade Commission (FTC) or state Attorney General. The FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft/, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The FTC also encourages those who discover that their information has been misused to file a complaint with them, and you can do so at www.identifytheft.gov. Identity theft should also be reported to your local law enforcement.

(5) *State-specific information.* **For Maryland residents,** the AG can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202, toll-free at 1-888-743-0023 or online at www.marylandattorneygeneral.gov. **For 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. Consumer reporting agencies must: (i) correct or delete inaccurate, incomplete, or unverifiable information, and they may not report outdated negative information; (ii) limit access to your file; (iii) get your consent before sharing your credit reports with employers; (iv) allow you to limit “prescreened” offers of credit and insurance based on your credit report. You may seek damages from violator. Identity theft victims and active duty military personnel have specific additional rights under the law (see www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or inquire with Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580). **For North Carolina Residents:** The North Carolina AG can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001, toll-free at 1-877-566-7226 and online at www.ncdoj.gov. **For Rhode Island Residents:** The Rhode Island AG can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 2 Rhode Island residents impacted by this incident.



* * *

We sincerely apologize for this incident and regret any inconvenience it may cause you. If you have questions, please contact the customer care team at **1-888-994-0277**.

Sincerely,

Scott Thompson, CEO
Astoria Company