

Return Mail Processing
PO Box 999
Suwanee, GA 30024

February 11, 2022

46 1 13333 *****SINGLP

SAMPLE A. SAMPLE - L02

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



NOTICE OF DATA BREACH

Dear Sample A. Sample:

On behalf of Ethos Technologies Inc. (“Ethos”), we are writing to inform you of a recent security incident where unauthorized actors may have accessed your driver’s license number. While we have no evidence to suggest that your driver’s license number has been misused, we are notifying potentially affected individuals and are providing them the opportunity to enroll in free credit monitoring.

What Happened? Ethos offers life insurance policies through an online application process. On January 12, 2022, we learned that unauthorized actors had launched a sophisticated attack against our online insurance application flow to access certain persons’ driver’s license numbers. We immediately began an investigation and took prompt action to prevent any further unauthorized access to this information.

Based on our investigation, to obtain your driver’s license number, the unauthorized actors needed to already have the following information about you, which they obtained from other sources: first and last name, date of birth, residential address, and driver’s license state of issuance. They then entered this information into our online insurance application flow to exploit a feature that validates applicant driver’s license numbers through a third-party service. Next, the unauthorized actors used specialized web tools to access driver’s license numbers from the page source code of our website. Importantly, this information did not appear on the public-facing parts of our website. The unauthorized activity spanned from approximately July 15, 2021 through January 12, 2022.

What Information Was Involved? Your driver’s license number.

What We Are Doing. We notified federal law enforcement and took prompt action to prevent any further unauthorized access to driver’s license numbers. These measures included technical changes to our website’s page source code. We also engaged an independent forensic investigation firm to assist our investigation of and response to this incident. These measures are in addition to those we have regularly maintained, which include penetration testing by internal and external security experts, annual cyber security audits, and threat prevention and detection software.

What You Can Do. We have arranged for you, at your option, to enroll in a free two-year credit monitoring and identity theft protection service. We have engaged Experian® to provide you with its IdentityWorksSM service, which includes credit monitoring, identity theft detection and resolution services, and up to \$1 million of identity theft insurance.¹ You must enroll by May 31, 2022 to activate this service by using the following activation code: ABCDEFGHI. This code is unique for your use and should not be shared. To enroll, visit <https://www.experianidworks.com/credit> or call (833) 671-0409. Please reference the following engagement number: B026792.

¹ 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.

Other Important Information. We also are providing you the following information about steps consumers can take to protect against potential misuse of information.

We urge you to remain vigilant for incidents of potential fraud and identity theft, including by regularly reviewing your account statements and monitoring your credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud or anything you do not understand, please call your financial institution(s).

In addition, you may contact the Federal Trade Commission (“FTC”) or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, contact the FTC by visiting www.ftc.gov/idtheft, calling 877-438-4338, or writing to the FTC’s Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. If you file a police report for identity theft, you should obtain a copy of such report as you may need to give copies of the report to others to remedy any fraudulent activity.

You may also periodically obtain a free copy of your credit report from each nationwide credit reporting agency (“CRA”). If you discover information on your credit report arising from a fraudulent transaction, you should request that the CRA delete that information from your credit report file. You are entitled to one free copy of your credit report every 12 months from each of the three CRAs. You may obtain a copy of your credit report by visiting www.annualcreditreport.com or by calling 1-877-322-8228. You may contact the CRAs at:

Equifax (www.equifax.com)

General Contact:

P.O. Box 740241, Atlanta, GA 30374
800-685-1111

Fraud Alerts and Security Freezes:

P.O. Box 740256, Atlanta, GA 30374

Experian

(www.experian.com)

General Contact:

P.O. Box 2104, Allen, TX
75013

888-397-3742

Fraud Alerts and Security

Freezes:

P.O. Box 9554, Allen, TX
75013

TransUnion

(www.transunion.com)

**General Contact, Fraud Alerts
and Security Freezes:**

P.O. Box 2000, Chester, PA
19022
800-916-8800

You may obtain additional information from the FTC and the CRAs about fraud alerts and security freezes. You can add a fraud alert to your credit report file at no cost to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three CRAs listed above. As soon as that CRA processes your fraud alert, it will notify the other two CRAs, which then must also place fraud alerts in your file.

You can also contact each of the CRAs at the numbers listed above to place a security freeze at no cost to restrict access to your credit report. You will need to supply your name, address, date of birth, Social Security number, and other personal information. After receiving your request, each CRA will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

You also have other rights under the Fair Credit Reporting Act (“FCRA”). For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

For More Information. For more information about this incident, or if you have questions or concerns, you may contact a dedicated team at (833) 671-0409 between the hours of 8 a.m. to 10 p.m. Central time, Monday through Friday (excluding major U.S. holidays), and from 10 a.m. to 7 p.m. Central time, on Saturday and Sunday.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ody Lupescu', written over a light grey circular watermark.

Ody Lupescu
Vice President of Security

