



Tiana Demas
T: +1 212 479 6560
tdemas@cooley.com

VIA EMAIL

December 20, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

On behalf of Ethos Technologies Inc. (“Ethos”), a life insurance provider, I write to inform you of a recent incident involving unauthorized access to Social Security numbers (the “Incident”).

Ethos offers life insurance policies through an online application process (the “Online Flow”). On December 8, 2022, Ethos learned that unauthorized actors had launched a sophisticated and successful cyberattack against the Online Flow to access certain persons’ Social Security numbers (“SSNs”). During the attack, the unauthorized actors entered information they had obtained from other sources—first and last name, address, and date of birth—into the Online Flow. Then they examined specific endpoints within the Online Flow’s page source code to access SSNs, which had been returned via a third-party integration.¹

Until August 2022, Ethos had encrypted all SSNs returned through this integration. However, in August 2022, Ethos made changes to its back-end code, which unintentionally caused SSNs to be returned to the front-end of the application in both unencrypted and encrypted formats. The unauthorized actors exploited the coding error by using specialized web tools to access the SSNs. They also took steps to avoid detection, including by conducting the attack at a slow rate to avoid Ethos’ rate limits. Importantly, the unencrypted SSNs did not appear on the site’s public-facing application page at any time. The unauthorized activity occurred between approximately August 4, 2022 and December 9, 2022.

Upon discovering the Incident, Ethos launched an investigation, promptly notified the FBI, and made a series of technical changes to the website’s software code. The changes were designed to prevent further unauthorized access to SSNs, and Ethos has not detected any unauthorized activity since December 9, 2022.

¹ Ethos uses this third-party integration as part of its identity validation and underwriting process. The integration allows Ethos to confirm the identities of insurance applicants for compliance and fraud detection purposes.



December 20, 2022
Page Two

On December 21, 2022, Ethos will begin notifying approximately 719 Maryland residents, who will be offered two years of free credit monitoring and identity theft protection services through Experian. The services can be activated until May 31, 2023.

Enclosed please find a sample notice letter to Maryland residents.

Should you have any questions, please contact me at tdemas@cooley.com or (212) 479-6560.

Sincerely,

A handwritten signature in black ink, appearing to read "T. Demas", is written over the typed name.

Tiana Demas

Encl.

December 21, 2022

126 1 33985
SAMPLE A. SAMPLE - L01



APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



Dear Sample A. Sample:

On behalf of Ethos Technologies Inc. (“Ethos”), we are informing you of a recent cyberattack in which unauthorized third-party actors may have accessed your Social Security number (“SSN”). We are offering you two years of free credit monitoring, identity theft protection services, and up to \$1 million of identity theft insurance¹ through Experian®.

What Happened? Ethos offers life insurance policies through an online application process. On December 8, 2022, we learned that unauthorized actors had launched a sophisticated and successful cyberattack against our website to access certain persons’ SSNs. We immediately investigated the incident and made a series of technical changes to our website to prevent further unauthorized access to SSNs. The vast majority of people affected by this incident were not existing Ethos customers.

To access SSNs, the unauthorized actors entered information they had obtained about you from other sources—first and last name, date of birth, and address—into our online insurance application flow. This caused a third-party integrated service to return your SSN to the page source code on our website. Then, the unauthorized actors used specialized tools to extract SSNs from the page source code of our website. Importantly, these SSNs did not appear on the public-facing application page of the site. The incident spanned from approximately August 4, 2022 through December 9, 2022.

What Information Was Involved? Social Security number.

What We Are Doing. We notified the FBI and made a series of technical changes to the software code of our website. The changes are designed to prevent further unauthorized access to SSNs. We also engaged an independent forensic investigation firm to assist with our investigation of and response to the incident. In addition, we regularly conduct penetration testing, undergo annual cyber security audits, and use threat prevention and detection software.

What You Can Do. You can enroll in free two-year credit monitoring and identity theft protection services provided by Experian®. 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 insurance¹. You must enroll by **May 31, 2023** and provide this activation code: ABCDEFGHI. This code is unique to you and should not be shared. To enroll, visit <https://www.experianidworks.com/credit> or call (800) 960-1799. Please reference the following engagement number: B082840.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ody Lupescu'.

Ody Lupescu
Vice President of Security, Ethos

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. Below, we provide 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 because you may need to give a copy 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 (800) 960-1799 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.

For District of Columbia Residents: You may obtain information about avoiding identity theft from the District of Columbia Attorney General's Office: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001, 202-727-3400, <https://oag.dc.gov/>.

For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. The mailing address for Ethos is 5001 Plaza on the Lake, Suite 305, Austin, TX 78746, and the general phone number is (415) 915-0665.

For Massachusetts Residents: You have the right to obtain a police report.

For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/internet/privacy-and-identity-theft>.

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

