



DLA Piper LLP (US)
4365 Executive Drive
Suite 1100
San Diego, California 92121-2133
www.dlapiper.com

Andrew Serwin
andrew.serwin@dlapiper.com
T 858.677.1418
F 858.638.5063

VIA EMAIL: idtheft@oag.state.md.us

May 9, 2024

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

Re: Security Incident Notification

Dear Sir or Madam:

We are providing notice on behalf of Allianz Global Risks U.S. Insurance Company (“Allianz”) of a data security incident suffered by a third-party service provider of Allianz, Enstar (US) Inc. (“Enstar”). Please be advised that Allianz understands that Enstar may have previously notified your office of this security incident, and on November 20, 2023, provided affected individuals, including Maryland residents, with a written notification of the incident. Nonetheless, Allianz is providing your office with this notification in an effort to comply with its legal obligations under your state’s security incident notification statute.

On May 31, 2023, Enstar suffered a security incident resulting from an exploited zero-day vulnerability in MOVEit, which is a widely used third-party file transfer tool owned by Progress Software and utilized by Enstar to send and receive data files. Enstar maintains Allianz data through Enstar’s capacity as a third-party service provider on behalf of Allianz Reinsurance America, Inc. (“AZRA”), which, in turn, is a third-party administrator/service provider for certain Allianz claims. The Enstar incident allowed an unauthorized third party to access Enstar’s file transfer server between May 29, 2023, and May 31, 2023, and exfiltrate data during that time. On November 20, 2023, Enstar provided all impacted individuals with a written notification of this security incident and notified AZRA that it had done so that same day. Subsequently, on November 21, 2023, AZRA informed Allianz of the security incident affecting information related to Allianz and its claimants (collectively, the “Allianz Data”) and that Enstar had already provided notification to those individuals it determined to be claimants of Allianz without identifying or describing its relationship to Allianz.

Upon receiving notice of the security incident, Allianz conducted its own investigation with the assistance of reputable third-party cybersecurity experts to confirm the nature of the impacted Allianz Data and whether the scope and methods of Enstar’s investigation were sound. On January 19, 2024, those third-party cybersecurity experts confirmed the extent of impact to Allianz claimants and that Enstar’s investigative methods were appropriate. As a result, and to ensure full disclosure of our involvement in this matter and relationship to Enstar, Allianz is providing your office with this notification.

The notification letter Enstar previously sent to affected residents on November 20, 2023 identified the specific data elements impacted for each individual who received notice.

The information involved varies by individual but generally includes one or more of the following types of personal information: Driver's License Number; Financial Account and Routing Number; Health Insurance Group / Plan Number, Policy Number, and Subscriber Number; Tax Payer Identification Number; Insurance Policy Number; Insurer Entity Name(s); Medicaid / Medicare Number; Medical Dates of Service; Medical History; Medical Provider Name; Medical Record Number; Medical Treatment / Procedure Information; Patient Account Number; Prescription Information; and Social Security Number.

In response to this incident and after receiving notice from Enstar, Allianz has taken steps to implement additional safeguards and reviewed its contracts, policies and procedures relating data privacy and security of its vendors, and in particular, Enstar.

As previously mentioned, on November 20, 2023, Enstar mailed written notice to affected residents and offered complimentary access to 24 months of credit monitoring and identity theft restoration services through Experian Consumer Services (also known as ConsumerInfo.com). Residents who received notice could have enrolled in the services at no cost by using a promotional code and instructions provided to them in the notification letter.

A sample notification letter previously mailed to residents by Enstar is enclosed.

Should you have any questions regarding this matter or if we can be of any further assistance to the residents affected by this incident, please contact me at (858) 677 1418 or Andrew.Serwin@us.dlapiper.com.

Respectfully submitted,

DLA Piper LLP (US)

Andrew Serwin

Enclosure: Sample Notification Letter



Enstar (US) Inc.

Return Mail Processing
PO Box 999
Suwanee, GA 30024

223 1 64886 *****AUTO**ALL FOR AADC 913

SAMPLE A. SAMPLE [Extra1] - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



November 20, 2023

RE: Notice of Data Privacy Event - reference [Internal ID]

Dear Sample A. Sample [Extra1]:

Enstar (US) Inc. ("Enstar" or "we") writes to notify you of an incident that may affect the privacy of some of your information. Enstar focuses on the acquisition and management of (re)insurance companies and portfolios of (re)insurance business from other insurance companies and groups. We have identified that this includes a company from whom you have either purchased a policy from or alternatively against whom you made an insurance claim as a result of suffering an injury or a financial loss. This letter includes details of the incident, our response, and steps you may take to better protect against possible misuse of your information, should you feel it appropriate to do so.

What Happened?

On May 31, 2023, Progress Software Corp. publicly disclosed a zero-day vulnerability that impacted the MOVEit Transfer tool. As a user of that tool, we moved quickly to apply all software updates provided by the vendor to address vulnerabilities associated with the application and undertook recommended mitigation steps. We promptly launched an investigation, with the assistance of third-party cyber forensic specialists, to determine the nature and scope of the potential impact of the vulnerabilities' presence on our MOVEit Transfer server and on the data it stored. Our investigation determined that an unauthorized actor (subsequently identified as the criminal group known as 'CLOP') exploited this zero-day vulnerability, accessed the MOVEit Transfer server between May 29, 2023, and May 31, 2023, and exfiltrated data over that time. We subsequently undertook a time-consuming and comprehensive review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates. On October 21, 2023, we completed this review and determined that data related to you was present on the impacted server at the time of the event.

What Information Was Involved? Enstar determined that the following information related to you was present within the accessible files: your name and the following elements: [Extra2][Extra3][Extra4].

What Enstar Is Doing. Enstar takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery, we immediately commenced an investigation to confirm the nature and scope of the incident. We reported this incident to law enforcement, and we are taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security.

As an added precaution, we are also offering you complimentary access to 24 months of credit monitoring and identity theft restoration services through Experian Consumer Services (also known as ConsumerInfo.com). We encourage you to enroll in these services; we are not able to act on your behalf to enroll you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. Enstar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You can also review the enclosed *Steps You Can Take to Protect Personal Information* for general guidance. In addition, you can enroll in the complimentary credit monitoring and identity protection services being offered through Experian Consumer Services (also known as ConsumerInfo.com).

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call 800-626-5042, Monday through to Friday from 9 am – 11 pm Eastern, or Saturday and Sunday from 11 am – 8 pm Eastern (excluding major U.S. holidays). You will be asked to provide your engagement number B107245.

We sincerely regret any inconvenience that this event may cause you.

Sincerely,

A handwritten signature in dark ink, appearing to read 'Richard Seelinger', with a stylized, flowing script.

Richard Seelinger
President and CEO Enstar US Inc.

Steps You Can Take to Protect Personal Information

Enroll in Credit Monitoring Services

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- **Visit** the Experian IdentityWorksSM website <https://www.experianidworks.com/credit> and follow the instructions provided to enroll
- Provide your **activation code when prompted: ABCDEFGHI**
- Ensure that you **enroll by: February 29, 2024** (Your code will not work after this date.)

If you have questions about setting up or activating your IdentityWorksSM membership, need assistance with the services provided or would like an alternative method of enrolling in Experian IdentityWorksSM please contact Experian's customer care team at 800-626-5042 by **February 29, 2024**.

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. Identity Restoration is available to you for 24 months 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.

Our call center is open from Monday through to Friday from 9 am – 11 pm Eastern, or Saturday and Sunday from 11 am – 8 pm Eastern (excluding major U.S. holidays). Be prepared to provide engagement number **B107245** as proof of eligibility for the identity restoration services by Experian.

Monitor Your Accounts

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 1-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. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/>.

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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 103 Rhode Island residents impacted by this incident.