



October 3, 2023

By Email

Idtheft@oag.state.md.us

Orrick, Herrington & Sutcliffe LLP

401 Union Street
Suite 3300
Seattle, WA 98101-2668

+1 206 839 4300

orrick.com

Joseph C Santiesteban

E jsantiesteban@orrick.com

D +1 206 839 4352

F +1 206 839 4301

RE: Notice of Security Event Relating to Maryland Residents / Sony Interactive Entertainment, LLC

Dear Attorney General,

I am writing on behalf of our client, Sony Interactive Entertainment, LLC ("SIE"), to notify you of a security event.

On May 31, 2023, Progress Software announced a newly discovered vulnerability in its MOVEit file transfer platform, which is used by SIE and thousands of other enterprises around the world. On May 28, 2023, before Progress Software announced the vulnerability, an unauthorized actor used the vulnerability to download some files stored on SIE's MOVEit platform, as part of a global attack on enterprises using the application. On June 2, 2023, SIE discovered the unauthorized activity, immediately took the platform offline and remediated the vulnerability. An investigation was then launched with assistance from external cybersecurity experts. SIE also notified law enforcement. The incident was limited to the MOVEit platform. Other SIE systems and services were not affected.

Once SIE was able to identify affected files, SIE began a process to determine who was affected and the types of information that were affected. This analysis was time consuming. SIE determined that the personal information of ten (10) Maryland residents who are current, former, or prospective SIE employees or employee dependents was in the downloaded files. Depending on the individual, the types of personal information that were downloaded include one or more of the following: address, email address, Social Security Number, telephone number, date of birth, salary and compensation information, and vaccination status. SIE is offering these individuals two years of complimentary credit monitoring and identity restoration services through Equifax.

SIE provided all employees initial information about the event on June 9, 2023 understanding that some employee personal information might be affected. Following the conclusion of the investigation, the company began notifying residents via U.S. First Class Mail on October 3, 2023. A sample notice is attached as Attachment A.



In addition to promptly remediating the vulnerability, SIE has increased the monitoring of its systems and is taking other steps to reduce the risk of this type of cyber event occurring in the future.

If your office requires any further information in this matter, please contact me at +1 (206) 839-4352 or at jsantiesteban@orrick.com.

Respectfully yours,

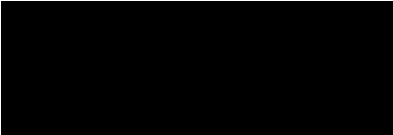
/s/ Joseph C. Santiesteban
Partner, Orrick Herrington & Sutcliffe LLP



Sony Interactive Entertainment
2540 Walden Avenue
Suite 450
Cheektowaga, NY 14225

October 3, 2023

000001



Re: Notice of Data Breach / Notice of Security Event



We are writing to you as we believe you are a former employee of Sony Interactive Entertainment (“**SIE**”) or are a family member of a current or former employee of SIE. We want to provide you with information about a cybersecurity event related to one of our IT vendors, Progress Software, that involved some of your personal information. This event was limited to Progress Software’s MOVEit Transfer platform and did not impact any of our other systems. Please read this notice carefully, as it provides information on what happened and what we are doing, as well as information on how you can obtain complimentary credit monitoring and identity restoration services.

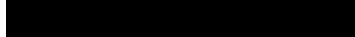
What happened?

On May 31, 2023, Progress Software announced a newly discovered vulnerability in its MOVEit file transfer platform, which is used by SIE and thousands of other enterprises around the world. On May 28, 2023, before Progress Software announced the vulnerability and we became aware of it, an unauthorized actor used the vulnerability to download some SIE files stored on our MOVEit platform. On June 2, 2023, SIE discovered the unauthorized downloads, immediately took the platform offline and remediated the vulnerability. An investigation was then launched with assistance from external cybersecurity experts. We also notified law enforcement.

What information was involved?

Once SIE identified the downloaded files, we began a process to determine what types of personal information were affected and to whom it relates. While we worked quickly, this was a time-consuming process, and we wanted to provide you accurate information.

Within the downloaded files, we identified the following information about you:



What we are doing:

In addition to immediately remediating the vulnerability, SIE has increased the monitoring of its systems and is taking other steps to reduce the risk of this type of cyber event occurring in the future.

While we are not aware of publication or misuse of your personal information identified in this letter, SIE is also offering complimentary Equifax Complete Premier credit monitoring and identity restoration services to you.

Please see [Attachment A](#) for details regarding these services.

[Attachment A](#) contains details of how to enroll with your unique code. **You must enroll by February 29, 2024, to receive these services.**

What you can do:

It is always a good idea to remain vigilant against threats of identity theft or fraud and to review and monitor your account statements and credit history for any signs of unauthorized transactions or activity regularly. If you ever suspect that you are the victim of identity theft or fraud, you can contact your local law enforcement. Additional information about how to protect your identity is contained in [Attachment B](#).

For more information:

SIE has established a dedicated call center to answer questions about the cybersecurity event as well as the Equifax services that we are offering to you. If you have any questions, please call the call center 1-855-457-8896 Monday through Friday from 9:00 a.m. to 6:00 p.m. ET.

Sincerely,

Sony Interactive Entertainment

Attachment A

Attachment B



Attachment A – Vendor Instructions



Enter Activation Code: [REDACTED]
Enrollment Deadline: **February 29, 2024**

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of [REDACTED] then click “Submit” and follow these 4 steps:

1. Register:

Complete the form with your contact information and click “Continue”.
*If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.
Once you have successfully signed in, you will skip to the Checkout Page in Step 4*

2. Create Account:

Enter your email address, create a password, and accept the terms of use.

3. Verify Identity:

To enroll in your product, we will ask you to complete our identity verification process.

4. Checkout:

Upon successful verification of your identity, you will see the Checkout Page.
Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.
Click “View My Product” to access the product features.

¹The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

²Credit monitoring from Experian and TransUnion will take several days to begin.

³WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded.

⁴The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ⁵Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.co

⁶The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Attachment B – Information for U.S. Residents

MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free +1 (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax	Experian	TransUnion
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft



ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

District of Columbia Residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; +1 (202) 727-3400; oag@dc.gov and www.oag.dc.gov

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319; +1 (515) 281-5164; www.iowaattorneygeneral.gov

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the cybersecurity event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (877) 566-7226 (Toll-free within North Carolina); +1 (919) 716-6400; or www.ncdoj.gov

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

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

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; +1 (877) 877-9392 (toll-free in Oregon); +1 (503) 378-4400; or www.doj.state.or.us/

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400; or <https://riag.ri.gov> You may also file a police report by contacting local or state law enforcement agencies. There are 3 Rhode Island residents impacted by this incident.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, D.C., and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

