Orrick, Herrington & Sutcliffe LLP
401 Union Street
Suite 3300
Seattle, WA 98101-2668
+1 206 839 4300
orrick.com

February 22, 2024

BY EMAIL
DOJ-CPB@DOJ.NH.GOV

To Whom It May Concern:

I am writing on behalf of our law firm client, Insomniac Games, a private company headquartered at 2255 N Ontario Street, Suite 550, Burbank, CA 91504, to provide notice of a security event.

On November 26, 2023, Insomniac Games identified that an unauthorized actor had accessed some of its IT systems. Immediately upon detection, Insomniac Games took steps to terminate the access, including taking certain systems offline. An investigation was then launched with assistance from external cybersecurity experts and the matter was reported to law enforcement.

Insomniac Games subsequently discovered the unauthorized actor exfiltrated files containing personal information between November 25 and November 26, 2023. Once Insomniac Games identified the downloaded files, it began analyzing the files to determine what types of personal data were affected and to whom it relates. This analysis was time consuming.

Insomniac Games recently determined that the personal information related to 3 New Hampshire residents was included within the exfiltrated files. The types of personal information that were in the affected files varies by individual but may have included:

.

Insomniac Games provided all employees initial information about the event on December 11, 2023 understanding that some employee personal information might be affected. Following the conclusion of the investigation, the company began notifying individuals on February 22, 2024, via U.S. First Class Mail and email. Insomniac Games is offering individuals of free credit monitoring and identity protection services from Equifax.

Prior to the incident, Insomniac Games had a number of cybersecurity measures in place. After becoming aware of this incident, Insomniac Games took steps to prevent further access to the impacted systems, including taking certain systems offline. As Insomniac Games brought systems back online, they took a series of steps to further strengthen their security controls.

A sample notice is attached as Attachment A to this letter. If you have any questions, please do not hesitate to contact me at or at

Respectfully yours,

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

Attachment A

Re: Notice of Data Breach

SAMPLE A. SAMPLE,

We want to provide you with an update to our December 11, 2023 message about the cybersecurity event at Insomniac Games ("Insomniac"). As you know, we store and maintain files containing employment information, including personal information about you. Unfortunately, these files were downloaded by an unauthorized actor and released online. We understand that this news may be upsetting, but we want to assure you that we take the security of your information very seriously.

We are sending you this notice because we have completed our analysis of the types of personal information that were impacted. Please read this notice carefully, as it provides up-to-date information on what happened, what information about you was involved, what we are doing, as well as information on how you can obtain complimentary credit monitoring and identity restoration services.

What happened?

Late last year, Insomniac identified that an unauthorized actor had accessed some of our IT systems and downloaded files, including files containing personal information. Immediately upon detection, we took steps to terminate the access, including taking certain systems offline. An investigation was then launched with assistance from external cybersecurity experts. We also notified law enforcement. No Sony systems were impacted.

What information was involved?

Once Insomniac identified the downloaded files, we began analyzing the files 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 with accurate information.

We recently determined that between November 25 and November 26, 2023, the unauthorized actor downloaded the following information about you: [variable text for data elements].

What we are doing:

We are committed to learning from this incident. We have strengthened our security controls and we are taking other steps to reduce the risk of this type of cyber event occurring in the future.

As you are aware, we offer ID Watchdog credit monitoring and identity restoration services to you during open enrollment as part of our employee benefit package. Insomniac and SIE are extending this package to of complimentary ID Watchdog credit monitoring and identity restoration services.

Please see Attachment A for details regarding these services.

If you have not yet enrolled to receive these services, Attachment A contains details of how to enroll. **You must enroll by to receive these services.**

If you have already enrolled to receive these services, you do not have to do anything. These services will be offered to you for two years in addition to your current enrollment period. Your access to these services will continue for two years even if you are no longer an Insomniac employee.

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:

We know that you may have questions or concerns. We encourage you to reach out to the dedicated call center we established to answer any questions you may have about the cybersecurity event. If you have any questions about the cybersecurity event, please call the call center 1-888-318-3922 Monday through Friday from 9:00 a.m. to 9:00 p.m. ET. If you have any questions about the ID Watchdog services, please contact ID Watchdog directly at 1-866-513-1518.

Thank you, as always, for your patience and understanding.

Sincerely,

Insomniac Games

Attachment A – Vendor Instructions

Ensure your data is adequately protected

We have reopened enrollment for ID Watchdog, an identity theft protection service offered through SIE Benefits for all US employees, including fixed-terms and interns. If you waived coverage in the past or were not previously eligible, we encourage you to sign up as soon as possible by completing the form here. This form will remain open until .

Unsure if you've previously elected coverage? Check

Please continue reading for next steps, depending on which population you fall into:

Previously Waived or Ineligible for Coverage (includes Fixed Terms and Interns)

Unsure if you've previously waived coverage? Check

You can sign up for coverage by completing the form here. ID Watchdog will send a registration link to your work email address to complete your enrollment. **This may take 2-3 business days from completion of the form.** Identity protection services will not be activated until you complete your enrollment using the registration link sent to you by ID Watchdog.

Elected, but Enrollment Not Complete

You may have previously elected ID Watchdog coverage during your new hire or Open Enrollment window, but did not complete the registration process. If you fall into this category, ID Watchdog will re-send the registration link to your work email address on Identity protection services will not activate until you complete your enrollment.

Actively Enrolled in ID Watchdog Coverage

Employees who have previously completed their ID Watchdog enrollment can access and manage their account directly at **https://www.idwatchdog.com/**.

Please contact ID Watchdog directly at for any registration or account issues. Certain accounts may require additional verification to be opened.

ID Watchdog services include credit and dark web monitoring, credit locks, and insurance and guaranteed resolution support in the event of identity theft. Details on complete ID Watchdog services are available on Nexus.

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

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 www.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 www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies. There is 1 Rhode Island resident impacted by this incident.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, 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).