NOTICE OF DATA BREACH

[SAMPLE]

Dear [SAMPLE]:

We value and respect the privacy of your personal information. We are writing to inform you of an incident which may involve some of your information, how we are actively addressing the situation, and what you should do to protect yourself.

What Happened: The Facts As We Currently Know Them: Late last week our servers were locked up due to a ransomware attack. We have been investigating the matter and restoring the servers. We recently became aware that at least some employee records stored on a company server were accessed by someone without authority to do so. We do not yet know for certain exactly how many employees' records were exposed, but we are sending this letter to all employees out of an abundance of caution.

What We Are Doing: We and our cyber forensics consultant are actively investigating the incident, working to restore our servers, and taking steps to prevent a recurrence. We have not been requested by law enforcement to delay this notification to you.

Types of Information Potentially Involved: At least the following types of personal information of at least some employees may have been accessed or copied: name, address, social security/national identity number, driver's license number, date of birth, financial and banking (e.g., direct deposit) information, health records, and other types of information.

What You Can Do & Steps You Should Take to Protect Yourself; More Information: Because JAKKS takes the protection of your personal information very seriously, we are arranging to provide twelve months of free credit monitoring services to all current and former employees of JAKKS. We will separately contact you with personalized information so that you can start the monitoring service. We recommend as initial additional steps that you freeze your credit with the main credit agencies, change your passwords for financial and other online accounts, and remain vigilant by reviewing account statements and monitoring free credit reports. We will shortly be sending you information on additional steps you can take to protect yourself.

Contact Information: For personnel-related questions, contact Elsa Morgan, SVP, Human Resources at hr@jakks.net or 424.268.9409.

We will notify you of additional relevant information as it becomes available. We sincerely apologize for any inconvenience this incident may cause. Be assured that we have been working, and will continue working, to protect the security and confidentiality of your information.

Sincerely,

Stephen Berman
President & CEO

IMPORTANT STEPS TO TAKE TO FURTHER PROTECT YOURSELF

IN THE UNITED STATES

Below are important steps you can take to protect your personal information:

1. Immediate Action. Run current anti-virus/malware software on your personal computers and external drives to which your JAKKS work computer may have been connected (e.g., by Wi-Fi or by cable) to reduce the risk of malware being on them. One such software for Windows-based computers is Windows Defender, which usually is pre-installed on all Windows computers.

2. Remain Vigilant. We recommend you remain vigilant for incidents of fraud and identity theft by obtaining and closely reviewing your credit card, bank, and other account statements and credit reports, and monitoring them periodically going forward.

3. Credit Monitoring. To help ensure that your information is not used inappropriately, JAKKS has contracted with a credit monitoring service for you to receive free credit monitoring for one year. We will separately contact you with personalized information to begin your monitoring.

4. Get a Copy of Your Credit Reports. You can obtain a free copy of your credit report, once every 12 months, from each of the major credit reporting agencies listed below by visiting http://www.annualcreditreport.com or calling 1-877-322-8228.

5. Report Any Fraudulent Activity. Report any fraudulent activity or any suspected identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). To file an FTC complaint about identity theft or learn more, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338).

6. Put a Credit Freeze on Your Credit File. You may be able to put a credit freeze (also known as a security freeze) on your credit file so that no new credit can be opened in your name without using a PIN number issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze, and using a credit freeze may delay your ability to obtain credit. You may incur a small fee (typically only a few dollars, and it's free in many states) to place, lift, and/or remove a credit freeze. Credit freeze laws, and the cost of placing, temporarily lifting, and removing a credit freeze, vary by state. Unlike a fraud alert (discussed below), you must separately place a credit freeze on your credit file at each of the four major credit reporting companies. The instructions for how to establish a credit freeze vary by state, so please contact the major credit reporting companies below for more information:

Equifax	https://www.equifax.com/personal/credit-report-services/credit-freeze/	800-525-6285	P.O. Box 105788, Atlanta, GA 30348
Experian	https://www.experian.com/freeze/center.html	888-397-3742	P.O. Box 9554, Allen, TX 75013
TransUnion	https://www.transunion.com/credit-freeze	800-680-7289	P.O. Box 2000, Chester, PA, 19022
Innovis	https://www.innovis.com/securityFreeze/index	800-540-2505	P.O. Box 1640, Pittsburgh, PA 15230

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above. A helpful resource for explaining how to place a credit freeze is at https://clark.com/credit/credit-freeze-and-thaw-guide/.

7. Place a Fraud Alert on Your Credit Report. We suggest you place a fraud alert on your credit report. An initial fraud alert lasting at least 90 days is free, and it informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the credit reporting agencies using the contact information above. The Federal Trade Commission website has guidance on this issue

at https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs. You can also contact them at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580 or by calling 1-877-ID-THEFT (1-877-438-4338).

8. Tax Return Information. If you suspect that a fraudulent tax return has or may be filed using your personal information, immediately contact the IRS and file a complaint. For more information, see https://www.irs.gov/uac/taxpayer-guide-to-identity-theft. If you receive a 5071C letter from the IRS indicating that there has been fraudulent activity, see the information at https://idverify.irs.gov/IE/e-authenticate/welcome.do. TurboTax also has good information at Identity Theft: What to Do if Someone Has Already Filed Taxes Using Your Social Security Number.