

JAKKS Pacific  
Return Mail Processing Center  
P.O. Box 3826  
Suwanee, GA 30024

<<MailID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<City>><<State>><<Zip>>  
<<Country>>

May 17, 2023

***RE: Important Security Notification***  
***Please read this entire letter.***

Dear <<Full Name>>:

We are contacting you to provide notice of a data security incident that impacted the personal information we store about you. This notice is designed to provide you with information regarding the steps we have taken to protect your information and tools you can utilize to protect your identity, including an offer of free credit monitoring.

**What We Are Doing to Secure Your Information:** JAKKS takes the privacy and security of your personal information seriously and its investigation of this incident is ongoing. JAKKS has retained expert third party cyber security, forensics, and legal counsel to help fully investigate and remediate the incident. JAKKS has coordinated with law enforcement in the investigation of this incident and law enforcement has not instructed JAKKS to delay notification.

**What You Can Do & Steps You Should Take to Protect Yourself:** JAKKS has arranged to provide 24 months of free credit monitoring services. As an additional step, we recommend that you freeze your credit with the main credit reporting agencies whose contact information is listed below, change your passwords for financial and other online accounts, and remain vigilant by reviewing account statements and monitoring free credit reports. Additionally, you have the right to obtain a police report. To learn more about the steps you can take to protect yourself, please see the "Additional Resources" section included with this letter. This section includes important guidance and information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file free of charge.

**Equifax Credit Monitoring:** We are offering 24 months of free credit monitoring services through membership in Equifax Credit Watch Gold. This product provides you with credit monitoring, daily access to your credit report, and more. A credit card is not required for enrollment. To learn more, including how to enroll, please see the attached enrollment instructions.

**Contact Information:** If you have any questions, please contact Elsa Morgan, SVP Human Resources by phone at 424.268.9409 or by email at [hr@jakks.net](mailto:hr@jakks.net).

Sincerely,

Elsa Morgan  
SVP, Human Resources  
JAKKS Pacific INC.

## 1. Enrolling in Complimentary 24-Month Credit Monitoring.



Enter your Activation Code: <ACTIVATION CODE>  
Enrollment Deadline: August 31, 2023

### Equifax Credit Watch™ Gold

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

#### Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications<sup>1</sup> 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 alerts<sup>2</sup>, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock<sup>3</sup>
- 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 theft<sup>4</sup>

#### Enrollment Instructions

Go to [www.equifax.com/activate](http://www.equifax.com/activate)

Enter your unique Activation Code of <ACTIVATION CODE> 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.

<sup>1</sup>WebScan 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. <sup>2</sup>The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. <sup>3</sup>Locking 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.com](http://www.optoutprescreen.com) <sup>4</sup>The 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.

## IMPORTANT STEPS TO TAKE TO FURTHER PROTECT YOURSELF

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 is usually pre-installed on all Windows computers. We also recommend that you take immediate action by updating any commonly used passwords or security questions and implementing additional security measures, such as two factor authentication, where available.
- 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](http://www.ftc.gov/idtheft) or call 1-877-ID-THEFT (1-877-4384338). You may also contact the FTC or the below referenced state agencies for more information about preventing identity theft. Additionally, residents of Massachusetts are entitled to obtain a police report.
- 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	<a href="https://www.equifax.com/personal/credit-report-services/credit-freeze/">https://www.equifax.com/personal/credit-report-services/credit-freeze/</a>	800-525-6285	P.O. Box 105788, Atlanta, GA 30348
Experian	<a href="https://www.experian.com/freeze/center.html">https://www.experian.com/freeze/center.html</a>	888-397-3742	P.O. Box 9554, Allen, TX 75013
TransUnion	<a href="https://www.transunion.com/credit-freeze">https://www.transunion.com/credit-freeze</a>	800-680-7289	P.O. Box 2000, Chester, PA, 19022
Innovis	<a href="https://www.innovis.com/securityFreeze/index">https://www.innovis.com/securityFreeze/index</a>	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.** 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 (1-877438-4338).
- 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](#).