

17724

# KONAMI

585 Konami Circle

Las Vegas, NV 89119

702.616.1400

September 8<sup>th</sup>, 2020

[REDACTED]

[REDACTED]

**Re: July Security Incident**

Dear [REDACTED],

I am writing to you about the ransomware attack that Konami Gaming, Inc. ("KGI") experienced at the beginning of July. We have been working with law enforcement and several outside experts to understand how it happened, and what impact it had on our IT systems. Their investigation is now complete.

We wanted to let you know that during the course of their investigation, our experts determined that some of your personal information was downloaded from the KGI network immediately before the attack. **Our experts have uncovered no evidence that your information has been misused.** However, we want to make sure you have the right resources at your disposal to take the appropriate precautions you feel are needed to protect your identity.

## **What Happened?**

A threat actor used compromised KGI login credentials to download files from the KGI network between June 28, 2020 and July 5, 2020, and then to deploy ransomware on July 5, 2020. Through analysis of logs and other available information, our experts were able to determine that your personal information was contained within those files. Searches by our experts did **not** uncover any of these files online.

## **What Information Was Available?**

The documents that contained your personal information may have included your social security number, driver's license number, passport number, or health insurance number. Please reach out to Jeanie Griese in our HR Department at [griese0720@konamigaming.com](mailto:griese0720@konamigaming.com) or 702.952.1533 if you would like to know what specific information was found.

## **What We Are Doing**

We have added some additional network requirements to strengthen the security of our environment. We will continue to vigilantly monitor access to our systems for unauthorized activity, and are committed to protecting the information we maintain here at KGI.

## **What You Can Do**

We have included some additional resources that are available to protect your identity. All of these are simple, effective ways to detect the unauthorized use of your identity. We are also offering you a complimentary, one year subscription to a credit monitoring service. Please refer to the attached enclosure to subscribe to this service.

Please do not hesitate to reach out to Jeanie or myself if you have any questions or concerns. I am really sorry this happened, and thank you for all you do at Konami Gaming.

Sincerely,

A handwritten signature in cursive script, appearing to read "Thomas A. Jingoli".

Thomas A. Jingoli  
EVP/COO  
KONAMI GAMING, INC.  
702-616-1400

Enclosures

## DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

Konami Gaming, Inc. is offering you a one-year, complimentary membership for IdentityWorks<sup>SM</sup>, a product offered by Experian<sup>®</sup>, to help with detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: December 31, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code:** [REDACTED]

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **December 31, 2020**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE<sup>™</sup>:** You receive Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year 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](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## ADDITIONAL WAYS TO PROTECT YOUR IDENTITY

**1. Review your Credit Reports.** It's always a good idea to periodically monitor your credit reports. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.

**2. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax Fraud Reporting  
1-800-525-6285  
P.O. Box 740241  
Atlanta, GA 30374-0241  
[www.equifax.com](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

**3. Place Security Freezes.** By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your Social Security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

**4. Monitor Your Accounts.** Monitoring your financial account statements is another way to detect fraudulent activity. We would encourage you to report anything that looks suspicious to the respective financial institution.

**5. You can obtain additional information** about the steps you can take to avoid identity theft and more information about fraud alerts and security freezes from the Federal Trade Commission (FTC). You may contact the FTC, Consumer Response Center at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

**6. You have the right to obtain any police report** filed regarding this incident. You also have the right to file and obtain a copy of a police report if you are the victim of identity theft.