



Nintendo of America Inc.
4600 150th Avenue NE
Redmond, WA 98052 U.S.A.

(425) 882-2040
1-800-535-5304
FAX (425) 558-7100

20140

<Date>

<Name>

<street address>

<City, State, zip>

At Nintendo, we take the protection of your personal information very seriously. To that end, we are sending you this notice to make you aware of a recent incident that involved your personal information.

What Happened?

At the end of 2020, several non-New York employees, and former employees, received notice from the New York Department of Taxation and Finance (the "NYDTF") that a personal tax audit had been opened for tax years 2015 and/or 2016. Upon learning of this incident, we immediately launched our own investigation and began working with our external payroll provider that handled Nintendo's employee payroll for these tax years. As a result of our investigation, we learned the full extent of employees that were impacted by this incident and that it was caused by the mere presence of a New York State-specific tax field on our payroll provider's payroll file.

What Information Was Involved?

Upon discovering that personal tax audits were opened for non-NY employees, we conducted a comprehensive investigation to determine the extent to which employee personal information was shared with the NYDTF. This investigation found that your name, Social Security number, and mailing address had been shared with the NYDTF.

Our investigation did not find any evidence that the information had been further disclosed to, or shared with, any other entity. However, it is important to remain vigilant in regularly reviewing and monitoring all of your credit history to guard against any unauthorized transactions or activity. **Attachment A** contains additional information about steps you can take to protect yourself against fraud and identity theft.

What We Are Doing.

We immediately reported the incident to the NYDTF and began working with them to resolve the matter at the organizational level. Through these efforts, the NYDTF has closed the personal tax audits that were opened for all those individuals that were impacted. Additionally, letters evidencing the closure of such personal tax audits have been sent to all impacted individuals. Finally, we are offering you and other affected employees complimentary credit monitoring and identity theft protection services. Please contact us by using the e-mail address below for more information on how to access, or sign up for, these complimentary services.

For More Information.

We sincerely apologize for any inconvenience or concern that this incident may have caused you. If you have any questions about this notice or the incident, please feel free to contact us at HRNotifications@noa.nintendo.com.

Sincerely,

Dave Gies
Director, Employee Services
Nintendo of America Inc.
425-882-2040

ATTACHMENT A

Additional Information

To protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, review your account statements, and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert, credit freeze, or credit lock on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your State's attorney general, or the Federal Trade Commission.

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 (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

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

Equifax:
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
1-888-766-0008
www.equifax.com

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
TransUnion LLC
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting 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.

To place a fraud alert, contact any of the three major credit bureaus listed above and request that a fraud alert be put on your file. The bureau that you contacted must notify the other two bureaus. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one, including you, can open a new account. As a result, 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.

To place a credit freeze, contact all three credit reporting bureaus listed above and provide the personal information required by each bureau to place a freeze, which may include:

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 the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

When you place a credit freeze, you will be provided a PIN to use to freeze or unfreeze your credit report. A credit freeze lasts until you lift or permanently remove it, although in some jurisdictions it will expire after seven years. The cost to place a credit freeze is typically between \$5.00 and \$10.00 each time you place a freeze, but may vary by jurisdiction. Certain jurisdictions may also permit a credit reporting agency to charge you similar fees to temporarily lift or permanently remove the freeze. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a credit freeze.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three credit bureaus listed above and complete a credit lock agreement. The cost of a credit lock varies by credit bureau, which typically charge monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, 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

The 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, State Attorney General, or the FTC.