



August 29, 2022

Via Email

Office of the Attorney General, Washington
SecurityBreach@atg.wa.gov

Orrick, Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, WA 98104

+1 206-839-4300
orrick.com

Aravind Swaminathan

E ASwaminathan@orrick.com
D +1 206-839-4340
F +1 206-839-4301

RE: Notice of Data Security Incident Relating to Washington Residents / Neopets, Inc.

Dear Sir or Madam:

We are writing on behalf of our client, Neopets, Inc. (“Neopets” or the “Company”), to notify you of a data security incident. On July 20, 2022, Neopets was alerted to activity indicating unauthorized access by a third party to its IT systems. The Company took immediate steps to shut down further access to the affected systems and has not seen any unauthorized activity since that time. Neopets also launched an investigation assisted by a leading forensics firm and engaged with law enforcement. On August 10, 2022, Neopets determined that the event resulted in unauthorized access to, and in some cases, download of, player information.

Neopets determined that for past and present Neopets players, affected information may include the data provided when registering for or playing Neopets, including name, email address, username, date of birth, gender, IP address, Neopets PIN, and hashed password, as well as data about a player’s pet, game play, and other information provided to Neopets. For players that played prior to 2015, the information also could have included non-hashed, but inactive, passwords. This information appears to have been accessed and potentially downloaded between January 3-February 5, 2021, or July 16-19, 2022. Neopets does not store users’ government issued identification numbers, bank account information, or payment card information.

Neopets is committed to safeguarding its players’ information. As part of its ongoing commitment to the safety and privacy of the Neopets player information in its care, Neopets reset players’ passwords and is working on adding multi-factor authentication to better safeguard access to players’ accounts. The Company has also enhanced the protection of its systems, including by further strengthening its network monitoring, authentication, and system protection.

Neopets previously communicated about this event to players on July 21, 2022, and August 1, 2022, via its website and social media channels. The Company began notifying Washington residents via substitute notice on August 29, 2022. The press release and website content are attached.

Office of the Attorney General, Washington

August 29, 2022

Page 2

Neopets will update your office once it has determined approximately how many Washington residents were affected. If your office otherwise requires any further information in this matter, please contact me at (206) 839-4340 or ASwaminathan@orrick.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Aravind Swaminathan", with a long horizontal stroke at the end.

Aravind Swaminathan

Partner

Orrick, Herrington, & Sutcliffe, LLP

August 29, 2022

Re: Notice of Data Breach

Neopets began updating individuals today through its communication channels regarding a data incident that may have affected players' information. Neopets previously communicated about this incident to players on July 21, 2022, and August 1, 2022. This notice provides details about the incident, our response, and available resources.

What Happened?

On July 20, 2022, Neopets was alerted to activity indicating unauthorized access by a third party to our IT systems. We took immediate steps to shut down further access to the affected systems and we have not seen any unauthorized activity since that time. We also launched an investigation assisted by a leading forensics firm and engaged with law enforcement. On August 10, 2022, Neopets determined that the event resulted in unauthorized access to, and in some cases, download of, player personal information.

What Information Was Involved?

After our investigation, we have determined that for past and present Neopets players, affected information may include the data provided when registering for or playing Neopets, including name, email address, username, date of birth, gender, IP address, Neopets PIN, hashed password, as well as data about a player's pet, game play, and other information provided to Neopets. For players that played prior to 2015, the information also could have included non-hashed, but inactive, passwords. This information appears to have been accessed and potentially downloaded between January 3-February 5, 2021, or July 16-19, 2022.

We do not store users' government issued identification numbers, bank account information, or payment card information.

What We Are Doing

Neopets is committed to safeguarding our players' personal information. As part of our ongoing commitment to the safety and privacy of the Neopets' player information in our care, we have reset players' passwords and are working on adding multi-factor authentication to better safeguard your account access. We have also enhanced the protection of our systems, including by further strengthening our network monitoring, authentication, and system protection.

What You Can Do

If you used your Neopets password on other websites, we recommend that you change your passwords for those accounts as well. In general, it is a good idea to use different passwords across different applications and choose strong passwords.

In addition to changing your passwords, we recommend you do the following:

- While we are not aware of any misuse of your information, it is always a good practice to remain vigilant against threats of identity theft or fraud, and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity. If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police. Additional information about how to protect your identity is below.
- Additionally, it is always a good idea to be alert for "phishing" emails by someone who acts like they know you or are a company that you may do business with and requests sensitive information over email, such as passwords, government identification numbers, or bank account information.

For U.S. residents, additional information about how to protect your identity is contained below.

For more information:

If you have questions regarding this notice, we invite you to reach out to us through our normal support channels or by calling 1-310-533-3400, or toll-free at 1-800-413-0526, with any questions or concerns you might have regarding this incident or the security of your account.

Sincerely,

Jim Czulewicz
President & CEO
Neopets

Information for U.S. Customers

MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

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

To request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security Number;
- Date of birth;
- If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
- Proof of current address such as a current utility bill or telephone bill; and
- 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.

California Residents: Visit the California Department of Justice's Privacy Unit (<https://oag.ca.gov/privacy>) for additional information on protection against identity theft.

District of Columbia Residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; ag@dc.gov, and www.oag.dc.gov.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023, or www.marylandattorneygeneral.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 (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/articles/pdf-096-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.

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.



Neopets Provides Notice of Data Breach

NEWS PROVIDED BY
Neopets
Aug 29, 2022, 16:00 ET

SHARE THIS ARTICLE



EL SEGUNDO, Calif., Aug. 29, 2022 /PRNewswire/ - Neopets today began updating individuals through its communication channels regarding a data incident that may have affected players' information. Neopets previously communicated about this incident to players on July 21, 2022, and August 1, 2022. This notice provides details about the incident, our response, and available resources. Additional information about this incident is also available on our website www.neopets.com.

What Happened?

On July 20, 2022, Neopets was alerted to activity indicating unauthorized access by a third party to our IT systems. We took immediate steps to shut down further access to the affected systems and we have not seen any unauthorized activity since that time. We also launched an investigation assisted by a leading forensics firm and engaged with law enforcement. On August 10, 2022, Neopets determined that the event resulted in unauthorized access to, and in some cases, download of, player personal information.

What Information Was Involved?

After our investigation, we have determined that for past and present Neopets players, affected information may include the data provided when registering for or playing Neopets, including name, email address, username, date of birth, gender, IP address, Neopets PIN, hashed password, as well as data about a player's pet, game play, and other information provided to Neopets. For players that played prior to 2015, the information also could have included non-hashed, but inactive, passwords. This information appears to have been accessed and potentially downloaded between January 3-February 5, 2021, or July 16-19, 2022.

We do not store users' government issued identification numbers, bank account information, or payment card information.

What We Are Doing

Neopets is committed to safeguarding our players' personal information. As part of our ongoing commitment to the safety and privacy of the Neopets' player information in our care, we have reset players' passwords and are working on adding multi-factor authentication to better safeguard your account access. We have also enhanced the protection of our systems, including by further strengthening our network monitoring, authentication, and system protection.

What You Can Do

If you used your Neopets password on other websites, we recommend that you change your passwords for those accounts as well. In general, it is a good idea to use different passwords across different applications and choose strong passwords.

In addition to changing your passwords, we recommend you do the following:

- While we are not aware of any misuse of your information, it is always a good practice to remain vigilant against threats of identity theft or fraud, and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity. If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police.
- Additionally, it is always a good idea to be alert for "phishing" emails by someone who acts like they know you or are a company that you may do business with and requests sensitive information over email, such as passwords, government identification numbers, or bank account information.

For more information:






If you have questions regarding this notice, we invite you to reach out to us through our normal support channels with any questions or concerns you might have regarding this incident or the security of your account. Additional information about this incident is also available on our website www.neopets.com.

About Neopets

Launched in 1999, Neopets.com has been the most popular virtual pet site for the past two decades. Through a variety of mini-games, an expansive world to discover, a burgeoning community, and a robust virtual economy, players can explore, interact and engage with other Neopians in the lore and storied history of Neopia. The Neopets Community, like the game itself, is distinct, bold, and energetic, and enhances the overall experience of Neopets.com. To learn more about Neopets, please follow us on Twitter, Facebook, and YouTube.

SOURCE Neopets


Contact Cision

 Cision Distribution 888-776-0942
from 8 AM - 9 PM ET
Chat with an Expert
Contact Us 
  

Products

Cision Communication Cloud®
For Marketers
For Public Relations
For IR & Compliance
For Agency
For Small Business
All Products

About

About PR Newswire
About Cision
Become a Publishing Partner
Become a Channel Partner
Careers
COVID-19 Resources
Accessibility Statement
Global Sites 

My Services

All New Releases
Online Member Center
ProfNet