PERKINSCOIE

1201 Third Avenue
Suite 4900
Seattle, WA 98101-3099

STATE OF NH
DEPT OF JUSTICE

2015 FEB 13 AM 11:52

February 10, 2015

State of New Hampshire
Department of Justice
Office of the Attorney General Joseph Foster
33 Capitol Street
Concord, NH 03301

Re: Notification of Security Breach

Dear Mr. Foster:

I am writing on behalf of Big Fish Games, Inc. to inform you of a recent security breach incident involving our online stores that may have affected 146 residents of your state. An unknown criminal installed malware that appears to have intercepted information when customers entered new payment details for purchases on the Big Fish website. Big Fish self-discovered the breach on January 12, 2015, and believes it to have affected payment details newly entered on their websites between December 24, 2014 and January 8, 2015. This breach may have resulted in the unauthorized access to name, address, and payment card information, including card number, expiration date, and CVV2 code. Customers who made purchases during the affected time period using a saved payment method from their profile are not believed to have been affected by this incident.

Big Fish has taken the necessary steps to remove the malware and prevent it from being reinstalled, and has retained security forensics firms to assist us in investigating the incident. We have also informed the payment card networks about this incident so that they may take appropriate action regarding the potentially affected accounts.

Please find a copy of the notification that will be sent to the affected individuals today.

Please contact me with any questions or concerns regarding this incident.

Sincerely,

333 Elliot Avenue West
Suite 200
Seattle, WA 98119

February 11, 2015

##|A7977-L05-0123456
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

I am writing to inform you of an incident we self-discovered on January 12, 2015, involving the theft of payment information from our online stores. An unknown criminal installed malware on the billing and payment pages of our websites that appears to have intercepted customer payment information. Your information may have been affected if you entered new payment details on our websites (rather than using a previously saved profile) for purchases between December 24, 2014 and January 8, 2015. Your name, address, and payment card information, including the card number, expiration date, and CVV2 code, may have been among the information accessed.

We have taken the necessary steps to remove the malware and prevent it from being reinstalled. We have reported the incident to and are cooperating with law enforcement. We have also informed the credit reporting agencies and payment card networks about this incident so that they may take appropriate action regarding your card account.

We value the trust and confidence of our customers, and take the protection of your information seriously. To help protect your identity, we are offering a **complimentary** one-year membership to Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: May 31, 2015** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/alert**
3. PROVIDE **Your Activation Code: ABCDEFGHIJKL**

If you have questions or need an alternative to enrolling online, please call (877) 534-7032 and provide engagement #: **PC91786.**

We also recommend that you monitor your payment account records for fraudulent transactions. If you suspect fraudulent activity, you can contact your local law enforcement agency, the attorney general of your state, or the Federal Trade Commission (600 Pennsylvania Avenue, NW, Washington, D.C. 20580; consumer.ftc.gov; 1-877-ID-THEFT). You can also contact Experian for fraud resolution assistance.

0123456

The credit reporting agencies also provide information on how to avoid identity theft and what to do if you believe your identity has been stolen. Although payment card information should not enable a third party to create new accounts in your name, you should be aware that you can limit new accounts by contacting the credit reporting agencies directly to put in place a fraud alert or a security freeze.

A7977-L05

- Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
- TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

If you have questions, please call (877) 534-7032 Monday - Friday 6am – 6pm Pacific Standard Time and Saturday - Sunday 8am – 5pm Pacific Standard Time, or contact us at Big Fish Games, 333 Elliott Avenue West, Seattle, WA 98119.

On behalf of Big Fish Games, we regret any inconvenience this may cause you.

Sincerely,

Chief Technology Officer
Ian Hurlock-Jones

Addendum

Information for North Carolina residents:

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-NO-SCAM
www.ncdoj.gov

Information for Maryland residents:

You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office:

Maryland Attorney General's Office
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

A7977-L05