

April 13, 2018

FILE NO: 47221.9

**Via Certified Mail**

Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 00301

**RECEIVED**  
**APR 16 2018**  
**CONSUMER PROTECTION**

To Whom It May Concern:

I am writing on behalf of Best Buy Co., Inc. (“Best Buy”) to notify you about a recent data security issue that affected certain Best Buy customers’ information. The issue occurred on the systems of one of Best Buy’s vendors, [24]7.ai, which provides the technology Best Buy uses in the customer service chat function found on its website. This issue did not affect Best Buy systems or physical Best Buy stores.

In late March 2018, Best Buy was notified that [24]7.ai had been the victim of a cyber intrusion in the fall of 2017. Based on an internal investigation, [24]7.ai found that malicious code was inserted in its software between September 26, 2017 and October 12, 2017. This code appears to have enabled an unauthorized party to access payment information of certain Best Buy customers who shopped on BestBuy.com between those dates. The affected information included cardholder names, addresses and payment card information (including payment card number, expiration date and security code). Best Buy believes no other customer information was affected by this cyber intrusion.

After learning of the issue, Best Buy quickly began working to identify the Best Buy customers who may have been affected. Best Buy understands that [24]7.ai engaged leading data security experts to assist with the investigation and confirm that the malicious code had been removed from its software and the unauthorized access had been stopped. Because of that, and changes Best Buy has made to how the [24]7.ai software operates on its website, Best Buy believes the malicious code no longer poses a risk to customers shopping on its website.

Best Buy publicly announced on April 5, 2018, that it was one of the several businesses whose customer information may have been affected by this cyber incident. Best Buy and [24]7.ai also have been coordinating with law enforcement authorities in their investigation.

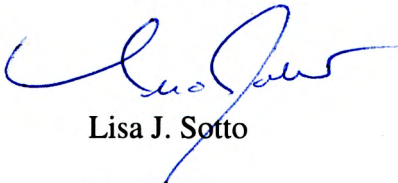
Best Buy is not able to determine at this time the number of Best Buy customers who are New Hampshire residents who may be affected by this issue. Best Buy has arranged to provide

Office of the New Hampshire Attorney General  
April 13, 2018  
Page 2

affected customers with identity theft services, including credit monitoring, at no cost for one year.

Attached for your reference is a copy of the notice that Best Buy is sending via postal mail to affected individuals. Please do not hesitate to contact me if you have any questions.

Very truly yours,



Lisa J. Sotto

Enclosure



P.O. Box 222455  
Chantilly, VA 20153-2455



April 12, 2018

First Name Middle Initial Last Name Suffix  
Address Line1  
Address Line2  
City, State Zip5-Zip4

### **NOTICE OF DATA BREACH**

Dear First Name Middle Initial Last Name Suffix,

There have been a number of recent media reports about a company called [24]7.ai that provides businesses like Best Buy with the technology we use in the customer service chat function found on our website. [24]7.ai recently told us they had been the victim of a cyber intrusion and theft in the fall of 2017, causing us to conduct a thorough review to identify customers who may have been affected by this crime. Regretfully, we have determined that your personal information may have been affected by this incident and we wanted to be sure you heard from us what happened and how we are prepared to help in response. Before we do this, we want to sincerely apologize for the trouble this incident may have caused you.

#### **What Happened?**

Based on an internal investigation, [24]7.ai found that malicious code was inserted in its software between September 26 and October 12, 2017. This code appears to have enabled an unauthorized party to access payment information of certain Best Buy customers who shopped on BestBuy.com between those dates. This issue did not affect Best Buy systems nor did it affect our physical Best Buy stores.

Best Buy publicly announced on April 5, 2018 that we were one of the businesses whose customer information may have been affected by this cyber incident.

#### **What Information Was Involved?**

The affected personal information included cardholder names, addresses and payment card information (including payment card number, expiration date and security code). We believe that no other customer information was affected by this cyber intrusion.

#### **What We Are Doing**

After learning of the issue, we quickly began working to identify the Best Buy customers who may be affected. We understand that [24]7.ai engaged leading data security experts to assist with the investigation and confirm that the malicious code had been removed from its software and the unauthorized access had been stopped. Because of that, and changes we have made to how the [24]7.ai software operates on our site, the malicious code no longer poses a risk to customers shopping on our website.

Product ID  
000001



## What You Can Do and How We Can Help

We know that you expect us to handle your information with great care and we take that obligation very seriously. We are alerting you about this issue so you can take steps to help protect yourself. Steps you can take include the following:

- Register for Identity Protection Services. We have arranged with Identity Guard®, to provide you with identity theft services, including credit monitoring, at no cost to you. Information about these services and instructions for enrollment are contained in the attached Reference Guide.
- Review Your Account Statements. We encourage you to remain vigilant by reviewing your payment card account statements. Please note: You are not liable for fraudulent charges that may result from this cyber intrusion, provided that you promptly report the charges to your credit card company. If you believe there are any unauthorized charges on your card as a result of this incident, please contact your card issuer as soon as you can.
- Order a Credit Report. U.S. residents are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit [annualcreditreport.com](http://annualcreditreport.com) or call toll-free at 1-877-322-8228.
- Review the Attached Reference Guide. The enclosed Reference Guide provides additional recommendations on the protection of personal information.

## For More Information

If you have any questions regarding this incident, please call us at 1-800-886-7983, 7:00 a.m. – 11:00 p.m. CDT, Monday-Sunday.

Again, please accept our apologies and know that we are here to help you.

Sincerely,



Steve Sissel  
Vice President, Enterprise Customer Care



## Reference Guide

We encourage our affected customers to take the following steps:

**Order Your Free Credit Report.** To order your free credit report, visit [annualcreditreport.com](http://annualcreditreport.com), call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at [consumer.ftc.gov](http://consumer.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

Here are some tips for reviewing your credit report: First, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number).

If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

**Register for Identity Theft Protection and Credit Monitoring Services.** We have partnered with Identity Guard to help you safeguard your identity and credit information for one year at no cost to you.

IDENTITY GUARD® TOTAL PROTECTION® features include:

- SSN Monitoring
- Online "Black Market" Monitoring
- ID Verification Alerts
- Account Takeover Alerts
- Identity Theft Victim Assistance
- Lost Wallet Protection
- Daily 3-Bureau Credit Monitoring
- 3-Bureau Credit Reports (Quarterly)
- 3-Bureau Credit Scores\* (Quarterly)
- ID Vault Password Protection
- Address Change Monitoring
- 3-Bureau Credit Analyzer
- \$1 Million Identity Theft Insurance\*\*
- Account Access via Mobile App
- Public Record Monitoring
- PC Keyboard Encryption Software
- PC Antivirus Software

If you wish to take advantage of this monitoring service, please enroll by July 24, 2018.

*\*The scores you receive with Identity Guard® are provided for educational purposes to help you understand your credit. They are calculated using the information contained in your Equifax®, Experian® and TransUnion® credit files. Lenders use many different credit scoring systems, and the scores you receive with Identity Guard are not the same scores used by lenders to evaluate your credit.*

Credit scores are provided by CreditXpert® based on data from the three major credit bureaus.

\*\*Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Product ID  
000001





**ENROLLMENT PROCEDURE:** To activate this coverage, please visit Identity Guard's Web site listed below and enter the redemption code. The redemption code is required for enrollment, and can only be used one time by the individual addressed.

Web Site: identityguard.com/bestbuy

Redemption Code: **Validation Codes**

In order to enroll, you will need to provide the following personal information:

- Mailing Address
- Phone Number
- Social Security Number
- Date of Birth
- E-mail Address
- Redemption Code

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel.

If you experience any issues or have questions while completing your online enrollment into Identity Guard® Total Protection®, please call 1-888-669-3238, 7:00 a.m. – 10:00 p.m. CDT, Monday-Friday or Saturday, 8:00 a.m. – 5:00 p.m. CDT.

**Report Incidents.** If you detect any unauthorized transactions in a financial account, promptly notify your credit (or debit) card issuer or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Place an initial fraud alert.
- Order your credit reports.
- Create a Federal Trade Commission Identity Theft Affidavit by submitting a report about the theft at [ftc.gov/complaint](http://ftc.gov/complaint).
- File a police report about the identity theft and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit with you when you file the police report.
- Your **Identity Theft Report** is your FTC Identity Theft Affidavit plus your police report. Your Identity Theft Report can be useful if you have any issues removing fraudulent information from your credit report, preventing companies from refurbishing fraudulent information to a consumer reporting agency, stopping a company from collecting a debt that resulted from identity theft, placing an extended seven-year fraud alert with consumer reporting agencies, and obtaining information from companies about accounts the identity thief opened or misused.

Product ID  
000001



You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[ftc.gov/idtheft/](http://ftc.gov/idtheft/)

**Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	transunion.com

**Consider Placing a Security Freeze on Your Credit File.** You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent, keeping them from opening any credit account in your name. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from \$5-\$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

**For Iowa Residents.** You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa  
Hoover State Office Building  
1305 E. Walnut Street  
Des Moines, IA 50319  
(515) 281-5164  
[www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)

**For Maryland Residents.** You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
(888) 743-0023 (toll-free in Maryland)  
(410) 576-6300  
[www.oag.state.md.us](http://www.oag.state.md.us)



**For Massachusetts Residents.** You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to \$5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

**For New Mexico Residents.** You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or [www.ftc.gov](http://www.ftc.gov).

**For North Carolina Residents.** You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
(877) 566-7226 (toll-free in North Carolina)  
(919) 716-6400  
[www.ncdoj.gov](http://www.ncdoj.gov)

**For Oregon Residents.** We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice  
1162 Court Street NE  
Salem, OR 97301-4096  
(877) 877-9392 (toll-free in Oregon)  
(503) 378-4400  
<http://www.doj.state.or.us>

**For Rhode Island Residents.** You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General  
Consumer Protection Unit  
150 South Main Street  
Providence, RI 02903  
(401)-274-4400  
<http://www.niag.ri.gov>

Product ID  
000001



You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to \$10 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.