

14513

#14513



<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> << NameSuffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

**Notice of Data Breach**

Dear <<FirstName>> <<LastName>>,

We are writing to notify you of a data security incident that occurred at Don Best Sports Corporation and DBS Canada Corporation (together, "Don Best") between October 12, 2018 and October 28, 2018, that involved an unauthorized disclosure of some of your personal information. The privacy and protection of our customers' information is a matter we take very seriously, and we have worked swiftly to resolve the incident. We deeply regret this incident and, as described below, we are taking steps to mitigate potential harm to you as a result of this incident.

**What Happened**

On November 1, 2018, Scientific Games Corporation ("Scientific Games") acquired Don Best. On December 21, 2018, while integrating the newly acquired Don Best network with that of Scientific Games, we learned that unauthorized individuals may have accessed the Don Best network. We immediately began an investigation and learned that between October 12, 2018 and October 28, 2018 Don Best suffered a malware attack.

**What Information Was Involved**

Based on Don Best's investigation to date, we believe that the unauthorized user accessed a Don Best database from which the unauthorized user accessed or acquired customer names, addresses, phone numbers, and usernames (which is a customer's e-mail address) and passwords. While the database at issue also stored credit card information, our investigation indicates that no credit card information was accessed or acquired.

**What We Are Doing**

Since becoming aware of this incident, Don Best has taken steps to remove the malware and to further improve the security of the Don Best network. Don Best is also resetting all customer passwords. Your trust is a top priority for Don Best, and we deeply regret the inconvenience this may cause.

**What You Can Do**

There are steps you can take to protect yourself, such as changing your password, placing a freeze on your credit report, or contacting the appropriate authorities if you believe you have been the victim of identity theft. The enclosed "Identity Theft Protection Tips" describes some of these steps. Of course, it is always important that you remain vigilant by reviewing your account statements and monitoring free credit reports for signs of fraud.

**For More Information**

To file a report of identity theft and to obtain more information about combating identity theft, you can contact the Federal Trade Commission at the phone number and address included in the enclosed "Identity Theft Protection Tips."

If you have any questions regarding this incident or about your accounts with Don Best, please contact the Service Center at [REDACTED], Monday through Friday between 9 a.m. and 6:30 p.m., Eastern Time.

Sincerely,

Don Best Sports Corporation

Enclosures: (1) Identity Theft Protection Tips  
(2) State Information

## Identity Theft Protection Tips

### *Change Your Passwords*

Because the information affected included your username or email address and password, we are prompting all Don Best customers to reset passwords for their Don Best accounts. You should also take steps appropriate to protect all online accounts that use the same username or email address and password. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to the relevant company that provides the account.

### *Monitor Your Accounts*

You should remain vigilant for incidents of fraud, identity theft, and errors by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

In addition, you are encouraged to contact the Federal Trade Commission (FTC), law enforcement, or your state attorney general to report incidents of suspected identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
(877) IDTHEFT (438-4338)  
[www.identitytheft.gov](http://www.identitytheft.gov)

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps, among others: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

### *Obtain Your Credit Reports*

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide consumer reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies. You may obtain a free copy of your credit report by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at <https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

Additionally, 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).

### *Place a Fraud Alert or Security Freeze on Your Credit File*

In addition, you may obtain information from the FTC and the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last one year. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide consumer reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. 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. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide consumer reporting agencies at:

Equifax  
P.O. Box 105788  
Atlanta, GA 30348  
(800) 525-6285  
[www.equifax.com](http://www.equifax.com)

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

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
(800) 680-7289  
[www.transunion.com](http://www.transunion.com)

### State Information

#### **IF YOU ARE AN IOWA RESIDENT:**

You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Iowa Attorney General  
Hoover State Office Building  
1305 E. Walnut Street  
Des Moines, IA 50319  
(515) 281-5926 / (888) 777-4590  
[www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)

#### **IF YOU ARE A MARYLAND RESIDENT:**

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
(888) 743-0023  
[www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov)

#### **IF YOU ARE A NORTH CAROLINA RESIDENT:**

You may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
(877) 566-7226  
[www.ncdoj.gov](http://www.ncdoj.gov)

#### **IF YOU ARE AN OREGON RESIDENT:**

You may report suspected identity theft to and obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at:

Oregon Department of Justice  
1162 Court Street NE  
Salem, OR 97301-4096  
(503) 378-4400  
[www.doj.state.or.us](http://www.doj.state.or.us)