Genesco Suffers Criminal Computer System Intrusion

December 10, 2010

NASHVILLE, Tenn., Dec. 10, 2010 /PRNewswire via COMTEX/ -- Genesco Inc. (NYSE: GCO) announced today that it suffered a criminal intrusion into the portion of its computer network that processes payment card transactions forits United States Journeys, Journeys Kidz, Shi by Journeys and Johnston & Murphy stores, and for some of its Underground Station stores. The Company took immediate steps to secure the affected part of its network, believes the intrusion has been contained and is confident that its customers can safely use their credit and debit cards in the Company's stores.

The extent of the intrusion is not known at this time. The Company is conducting a full investigation with the assistance of an outside expert to seek to determine the extent of any possible compromise of customer informationthat occurredin the intrusion. It is possible that the credit or debit card number, expiration date and card verification code contained on the magnetic stripe of some payment cards used at stores in the affected chains may have been acquired without authorization during the intrusion. The Company currently has no reason to believe that personal information, such as names, addresses or Social Security numbers, was acquired by the intruder. Additionally, the Company has no reason to believe that payment card transactions in any of its e-commerce or catalog businesses, any of its Lids Sports businesses, or any of its Canadian stores were affected by the intrusion.

The Company has notified law enforcement authorities and is cooperating in law enforcement's efforts to identify those responsible for the intrusion. The Company has also notified the major payment card brands and is cooperating in their investigation of the intrusion.

Genesco Chairman, President and Chief Executive Officer Robert J. Dennis said, "Since we learned of the intrusion, we have worked diligently with outside experts to protect our customers' information and we are confident that they are safe shopping with their credit and debit cards at our stores. We recommend that our customers review their card statements and other account information carefully and immediately notify their card issuer if they suspect fraudulent use. We sincerely regret any inconvenience this attack on our network may cause our customers."

Attached is a letter from Mr. Dennis that provides more information about the intrusion and additional steps customers can take to protect their information. The Company has also set up a toll-free hotline at (877) 441-2998 for customers who have further questions. The letter and the toll-free number are available on the Company's website at www.genesco.com/customerassistance.

Cautionary Note Concerning Forward-Looking Statements

This release contains forward-looking statements, including thoseindicatingexpectations about thefindings ofthe continuing investigation on topics includingthe timing and extent of the intrusion, and all other statements not addressing solely historical facts or present conditions. Actualevents and their consequences could vary materially from the expectations reflected in these statements. A number of factors could cause differences. These include results and effects of the intrusion, including the cost and outcome of our investigation, the results and effects that any breach could have on our customers, our sales and results of operations, and the cost and outcomes of any legal, regulatory or other actions brought against the Company by any private or public parties. Additional factors are cited in the "Risk Factors," "Legal Proceedings" and "Management's Discussion and Analysis of Financial Condition and Results of Operations" sections of, and elsewhere, in our SEC filings, copies of which may be obtained from the SEC website, www.sec.gov, or by contacting the investor relations department of Genesco via our website, www.genesco.com. Many of the factors that will determine the outcome of the subject matter of this release are beyond Genesco's ability to control or predict. Genesco undertakes no obligation to release publicly the results of any revisions to these forward-looking statements that may be made to reflect events or circumstances after the date hereof or to reflect the occurrence of unanticipated events. Forward-looking statements reflect the expectations of the Company at the time they are made. The Company disclaims any obligation to update such statements.

A Message From Genesco CEO Robert J. Dennis

December 10, 2010

Dear Customer:

Genesco recently became aware of a criminal intrusion into the portion of its computer network that processes payment card transactions for its United States Journeys, Journeys Kidz, Shi by Journeys and Johnston & Murphy stores, and for some of its Underground Station stores. Immediately upon learning of the intrusion, we took steps to secure the affected part of our network. We believe that the intrusion has been contained and are confident that our customers can safely use their credit and debit cards in all of our stores.

The Company has notified law enforcement authorities and is cooperating in law enforcement's efforts to identify those responsible for the intrusion. The Company has also notified the major card brands of the intrusion.

The extent of the intrusion is not known at this time. The Company is continuing to investigate the intrusion, with the assistance of an outside expert, in an effort to determine the extent of any possible compromise of customer information. It is possible that the credit or debit card number, expiration date and card verification code contained on the magnetic stripe of some payment cards used at the chains mentioned above may have been acquired without authorization during the intrusion. We currently have no reason to believe that personal information, such as names, addresses or Social Security numbers, was acquired by the intruder.

We recommend that customers review their card statements and other account information carefully and immediately notify their card issuer if they suspect fraudulent use. Because we have no reason to believe customers' personal information was compromised, we do not believe that identify theft is likely as a consequence of the intrusion. Nonetheless, we are providing the Reference Guide below, which details some steps you can take to

protect your personal information. For more information or with questions, please call our Customer Information Center at (877) 441-2998or write to me at1415 Murfreesboro Road, Suite 490, Nashville, TN 37217.

We sincerely regret any inconvenience this attack on our network may cause you. As always, we appreciate your choosing to shop in our stores.

Sincerely,

Robert J. Dennis

Chairman, President and Chief Executive Officer

Genesco Inc.

Reference Guide

In addition to carefully reviewing your financial institution and payment card statements, Genesco recommends you consider these additional steps:

Security Freeze. Some state laws allow you to place a security freeze on your credit reports. This would prohibit a credit reporting agency from releasing any information from your credit report without your written permission. You should be aware, however, 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. The specific costs and procedures for placing a security freeze vary by state law, but this reference guide provides general information. You can find additional information at the websites of any of the three credit reporting agencies listed below.

If you believe that you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it will not charge you to place, lift or remove a security freeze on your credit reports. In all other cases, a credit reporting agency may charge you up to $5.00 (and in some cases, up to $20.00) each time you place, temporarily lift, or permanently remove a security freeze.

Requirements vary by state, but generally to place a security freeze on your credit report, you must send a written request to each of the three credit reporting agencies noted below, which must include the following information: (1) Full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security Number; (3) Date of birth; (4) Addresses for the prior five years; (5) Proof of current address; (6) A legible copy of a government issued identification card; (7) A copy of any relevant 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, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash though the mail.

Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348 877-478-7625 www.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, Texas 75013 888-397-3742 www.experian.com	TransUnionFraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790 800-680-7289 www.transunion.com

Free Credit Reports. To order a free copy of your credit report, visitwww.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website atwww.ftc.govand mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three national credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, 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 credit bureau 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 credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus 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 credit bureau by telephone and in writing.

Fraud Alerts. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert alerts you of an attempt by an unauthorized person to open a new credit account 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 free fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus. You can also place a fraud alert on your credit report online at the websites listed below for Equifax and Experian and via email for TransUnion at fvad@transunion.com.

Equifax P.O. Box 105069 Atlanta, Georgia 30348-5069 800-525-6285 www.fraudalerts.equifax.com	Experian P.O. Box 1017 Allen, Texas 75013 888-397-3742 www.experian.com	TransUnionFraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790 800-680-7289 www.transunion.com

Police Report. If you find suspicious activity on your credit reports or account statements, or have reason to believe that your personal information is being misused, contact your local law enforcement authorities immediately and file a police report. You have the right to request a copy of the police report and should retain it for further use, as many creditors want the information it contains to absolve you of potential fraudulent debts.

Consulting the FTC. In addition to your state Attorney General, you can contact the FTC to learn more about how to protect yourself from identity theft:

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

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

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 can 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

SOURCE: Genesco Inc.