Letter from our local President

September 2, 2014

Dear Goodwill® Customers:

In July, Goodwill Industries International (GII), on behalf of its members, announced that some Goodwill members' store locations may have been affected by a data security issue. Since that time, we have engaged a third-party forensic expert to conduct an extensive investigation. We have also been working closely with federal law enforcement authorities and coordinating with the payment card brands to determine the facts.

The forensic investigation has confirmed that a third-party vendor's systems had been attacked by malware, enabling criminals to access some payment card data of a number of the vendor's customers. We want you to know that we have taken steps to secure our customers' data and we have stopped using the affected vendor to process our customers' payment cards. We also took immediate action to ensure the malware found on the third-party vendor's systems does not present a threat to individuals shopping at our stores.

Based on the investigation, we have determined the following:

- Twenty Goodwill members that use the same affected third-party vendor have been impacted.
- The investigation found no evidence of malware on any internal Goodwill systems.
- The third-party vendor's affected systems contained payment card information, such as names, payment card numbers and expiration dates, of certain Goodwill customers. There is no evidence that other Goodwill customer personal information, such as addresses or PINs, was affected by this issue.
- The malware attack affected the vendor's systems between February 10, 2013 and August 14, 2014. It affected our Goodwill stores between **June 25, 2013**, and **August 14, 2014** Click here for a list of all our local stores that used the affected vendor during the relevant time period.

We deeply regret any inconvenience this may cause. Our primary concern is for the people we serve — our community, our shoppers and our donors — and we are committed to ensuring that your information is safe and secure. We realize that data security is an issue that every retailer and consumer needs to be more and more aware of today.

We are notifying our customers about this issue so they can take steps to help protect their information. You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. If you believe your payment card may have been affected, please contact your bank or card issuer immediately. Additional information and security tips are available here.

If you have any questions or would like more information, please call us toll-free at 1-800-GOODWILL. We will be available to answer your questions from 9 a.m.-9 p.m. on Saturdays; 10 a.m.-7 p.m. on Sundays; and 9 a.m.-9 p.m. on Mondays-Fridays Eastern time.

Protecting the privacy of our customers' data information is extremely important to us, and we are diligently taking steps to help prevent this type of incident from occurring in the future. Again, we are very sorry this happened and we thank you for your continued support in helping Goodwill meet its mission of helping people with barriers to employment achieve economic independence for themselves and their families.

Sincerely,

Joseph R. Mendez

President

GOODWILL	ADDRESS	CITY	STATE	ZIPCODE	Exposure Start	Exposure End
CALIFORNIA						
SACRAMENTO, CA	6648 Franklin Blvd	Sacramento	CA	95823	1/27/2014	8/14/2014
SACRAMENTO, CA	2265 Arden Way	Sacramento	CA	95825	8/6/2013	8/14/2014
SACRAMENTO, CA	2460 Grass Valley Hwy	Auburn	CA	95603	8/15/2013	8/14/2014
SACRAMENTO, CA	4126 Manzanita Ave	Carmichael	CA	95608	7/30/2013	8/14/2014
SACRAMENTO, CA	7120 Auburn Blvd	Citrus Heights	CA	95610	7/30/2013	8/14/2014
SACRAMENTO, CA	4040 Florin Rd	Sacramento	CA	95823	6/25/2013	8/14/2014
SACRAMENTO, CA	8031 Watt Ave	Antelope	CA	95843	8/19/2013	8/14/2014
SACRAMENTO, CA	390 Plaza Dr	Folsom	CA	95630	8/13/2013	8/14/2014
SACRAMENTO, CA	3065 W Capitol Ave	West Sacramento	CA	95691	7/25/2013	8/14/2014
SACRAMENTO, CA	1312 Fulton Ave	Sacramento	CA	95825	8/6/2013	8/14/2014
SACRAMENTO, CA	1617 Douglas Blvd	Roseville	CA	95661	8/1/2013	8/14/2014
SACRAMENTO, CA	9400 Fairway Dr	Roseville	CA	95678	8/19/2013	8/14/2014
SACRAMENTO, CA	2502 Watt Ave	Sacramento	CA	95821	8/8/2013	8/14/2014
SACRAMENTO, CA	7441 W Stockton Blvd	Sacramento	CA	95823	7/23/2013	8/14/2014
SACRAMENTO, CA	5400 Date Ave	Sacramento	CA	95841	1/29/2014	8/14/2014
SACRAMENTO, CA	1621 L St	Sacramento	CA	95814	7/18/2013	8/14/2014
SACRAMENTO, CA	1643 Hilltop Dr	Redding	CA	96002	8/27/2013	8/14/2014
SACRAMENTO, CA	11092 Coloma Rd	Rancho Cordova	CA	95670	8/8/2013	8/14/2014
SACRAMENTO, CA	1640 E 8th St	Davis	CA	95616	7/18/2013	8/14/2014
SACRAMENTO, CA	765 East Ave Ste 100	Chico	CA	95926	8/22/2013	8/14/2014
SACRAMENTO, CA	120 Main St	Woodland	CA	95695	8/13/2013	12/30/2013
SACRAMENTO, CA	3615 Elkhorn Blvd	North Highlands	CA	95660	8/1/2013	8/14/2014
SACRAMENTO, CA	1242 Colusa Avenue	Yuba City	CA	95991	7/23/2013	8/14/2014

REFERENCE GUIDE

We encourage affected customers to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.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 www.consumer.ftc.gov and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies 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 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 can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company 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:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

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)
www.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	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	www.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. 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 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 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

FOR IMMEDIATE RELEASE
September 2, 2014

GOODWILL® PROVIDES UPDATE ON DATA SECURITY ISSUE

ROCKVILLE, MD — Goodwill Industries International (GII) today provided an update on behalf of its members regarding the potential data security issue it previously announced in July. Following GII's announcement, GII and the potentially affected Goodwill members engaged a third-party forensic expert to conduct an extensive investigation. GII and its members have also been working closely with federal law enforcement authorities and coordinating with the payment card brands to determine the facts.

The forensic investigation has confirmed that a third-party vendor's systems were attacked by malware, enabling criminals to access some payment card data of a number of the vendor's customers. The impacted Goodwill members used the same affected third-party vendor to process credit card payments. Each of the impacted Goodwill members took immediate action to ensure that the malware found on the third-party vendor's systems no longer presents a threat to individuals shopping at the affected Goodwill members' stores.

Based on the investigation, GII and its members have determined the following:

- Twenty Goodwill members (representing about 10 percent of all stores) that use the same affected thirty-party vendor were impacted.
- The investigation found no evidence of malware on any internal Goodwill systems.
- The third-party vendor's affected systems contained payment card information, such as names, payment card numbers, and expiration dates of certain Goodwill members' customers. There is no evidence that other customer personal information, such as addresses or PINs, was affected by this issue.
- The malware attack affected the third-party vendor's systems intermittently between February 10, 2013, and August 14, 2014. Some stores experienced shorter periods of impact. A list of the Goodwill members' store locations that used the affected vendor during the relevant time period is available on GII's website at http://www.goodwill.org/payment-card-notice.
- Goodwill members have received a very limited number of reports from the payment card brands of fraudulent use of payment cards connected to Goodwill members' stores.

"We continue to take this matter very seriously. We took immediate steps to address this issue, and we are providing extensive support to the affected Goodwill members in their efforts to prevent this type of incident from occurring in the future," said Jim Gibbons, president and CEO of Goodwill Industries International. "We realize a data security compromise is an issue that every retailer and consumer needs to be aware of today, and we are working diligently to prevent this type of unfortunate situation from happening again. Goodwill's mission is to provide job training for people with disabilities and disadvantages. We provide this service to millions of people each year. They, our shoppers and our donors, are our first priority."

Additional information related to this issue and steps that affected Goodwill members' customers can take to help protect their information is available on the GII website at http://www.goodwill.org/payment-card-notice

About Goodwill Industries International
Goodwill Industries International is a network of 165 community-based agencies in the United States and Canada with a presence in 14 other countries. Goodwill agencies are innovative and sustainable social enterprises that fund job training programs, employment placement services and other community-based programs by selling donated clothing and household items in their stores and online at *shop*goodwill.com®. Goodwill also builds revenue and creates jobs by contracting with businesses and government agencies to provide a wide range of commercial services, including packaging and assembly, food service preparation, and document imaging and shredding. In 2013, more than 9.8 million people in the United States and Canada benefited from Goodwill's career services.

CONTACT:
Lauren Lawson-Zilai
Director, Public Relations
Goodwill Industries International
Phone: (240) 333-5266
Lauren.Lawson@goodwill.org