Important Customer Notice

Information Concerning Data Security Incident at Some Staples Stores

Staples wants to make customers aware that we have confirmed a data security incident involving customer payment card data from purchases made at some of our U.S. retail stores. This notice explains what happened, describes the actions we've taken, and provides additional information and resources to anyone who may have been affected.

Staples' data security experts detected that criminals deployed malicious software, or "malware," to point-of-sale systems at 115 of its more than 1,400 U.S. retail stores. Upon detection, Staples immediately took action to eradicate the malware in mid-September and to further enhance security. Staples also retained outside data security experts to investigate the incident and has worked closely with the payment card companies and law enforcement on this matter.

Based on the investigation, Staples believes that malware may have allowed access to some transaction data at affected stores, including cardholder names, payment card numbers, expiration dates, and card verification codes. At 113 stores, the malware may have allowed access to this data for purchases made from August 10, 2014 through September 16, 2014. At two stores, the malware may have allowed access to data from purchases made from July 20, 2014 through September 16, 2014.

As a result, and in light of Staples' commitment to protecting its customers, Staples is offering free identity protection services, including credit monitoring, identity theft insurance, and a free credit report, to those customers who used a payment card at one of the affected stores during the relevant time periods. Additional information about the incident, including dates of potential access and how to sign up for free credit monitoring, can be found below.

In addition, during the investigation Staples also received reports of fraudulent payment card use related to four stores in Manhattan, New York at various times from April through September 2014. The investigation found no malware or suspicious activity related to the payment systems at those stores. However, out of an abundance of caution, Staples is offering free identity protection services, including credit monitoring, identity theft insurance, and a free credit report, to customers who used their payment cards at those stores during specific time periods.

Specific stores and dates can be found here.

Staples is committed to protecting customer data and regrets any inconvenience caused by this incident. Staples has taken steps to enhance the security of its point-of-sale systems, including the use of new encryption tools.

Toll-Free Call Center

Staples has established a toll-free call center, with operators standing by to address customer questions and concerns about this incident. Customers can call (866) 274-4371 – Monday through Friday: from 9:00 a.m. to 9:00 p.m. EST, and Saturday and Sunday: from 11:00 a.m. to 8:00 p.m. EST.

Identity Protection and Credit Monitoring Services

Because of our commitment to our customers, we are offering free identity protection services, including credit monitoring, for one year to any individuals who used a payment card at one of the affected stores during the specified time periods. Details of the services, which are provided by Experian, are available at www.protectmyid.com/staples.

Protecting Your Identity and Preventing Fraud

As a precaution, we encourage you to monitor your payment card account activity and immediately contact your bank or card issuer if you notice any unusual or suspicious activity. Typically, customers are not responsible for any fraudulent charges on their credit cards that are reported in a timely fashion.

If you detect any incident of identity theft or fraud, promptly report it to law enforcement or your state's Attorney General. If you believe your identity has been stolen, the U.S. Federal Trade Commission (FTC) recommends that you take these additional 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 may obtain additional information about identity theft and fraud alerts from the FTC. The FTC encourages those who discover that their information has been misused to file a complaint with the Commission. To do so, or to obtain additional information about identity theft and the steps that you can take to avoid it, you may contact the FTC at:

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

You also should monitor your credit reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228. You also may complete the Annual Credit Report Request Form, available on the FTC's website, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Alternatively, you can contact any of the three major credit reporting bureaus to request a copy of your credit report.

You also may request that the credit reporting bureaus place a "fraud alert" on your file at no charge. A fraud alert requires creditors to take additional steps to verify your identity prior to granting credit in your name for a 90-day period. Please note, however, that these additional verification steps may delay an approval of credit. If you wish to place a fraud alert, or if you

have questions about your credit report, you may contact any one of these credit reporting bureaus for information by using the contact information below:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

As discussed in more detail below, you also can contact the credit reporting bureaus for information on how to place a "security freeze" on your credit report that prohibits the bureaus from releasing information from your credit report without your prior written authorization.

Staples will never ask for your personal information in an email. If you elect to take advantage of the free identity protection services we are offering, you may be asked to provide your personal information to sign up for that service. If you have any questions about the authenticity of a communication you receive, please call 866-274-4371.

Your state also may offer guidance about how you can prevent or respond to identity theft. In particular, you may report instances of identity theft to your state's Attorney General or to your local police or sheriff's department. Contact information for some states appears below.

Attorney General's Office
California Department of Justice
Attn: Office of Privacy Protection
P.O. Box 944255
Sacramento, CA 94244-2550
Telephone: (916) 322-3360
Toll-free in California: (800) 952-5225

Director of Consumer Protection Division
Iowa Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
Telephone: 515-281-5926
www.iowaattorneygeneral.gov

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Telephone (toll-free): (888) 743-0023
E-mail: Idtheft@oag.state.md.us
www.oag.state.md.us

Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6000
Toll Free in NC: (877) 566-7226
FAX: (919) 716-6050
http://www.ncdoj.com

***For Massachusetts residents*:** Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Staples is cooperating with law enforcement to investigate the incident and identify those responsible.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. 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.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified, or overnight mail at the addresses below:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 95542	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);

2. Social Security Number;

3. Date of birth;

4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;

5. Proof of current address such as a current utility bill or telephone bill;

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);

7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;

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 through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) *and* the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days

after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) *and* the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.