BakerHostetler

Baker&Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com
Theodore J. Kobus III
direct dial: 212-271-1504
tkobus@bakerlaw.com

December 19, 2014

VIA OVERNIGHT DELIVERY

Iowa Attorney General
Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319

Re: Incident Notification

Dear Sir or Madam:

Our client, Staples, Inc. ("Staples"), is committed to protecting the payment card information of its customers. We are writing to inform you about an incident related to some of that information.

Staples self-detected malware activity in mid-September 2014 on some of the point-of-sale systems at a small percentage of its U.S. retail stores. Upon discovery, Staples immediately took steps to eradicate the malware. Staples also commenced an investigation, and worked closely with the payment card companies and law enforcement on the matter. In mid-December, 2014, the investigation found that the malware may have enabled an unauthorized person to access some payment card transaction data, possibly including cardholder names, payment card numbers, expiration dates, and card verification codes, at the affected point-of-sale systems for purchases made from August 10, 2014 through September 16, 2014. One store in your state was affected.

Staples is notifying all individuals who used a payment card at an affected store during the relevant time period and is offering these individuals free identity protection services from Experian, including credit monitoring, identify theft insurance, and a free credit report. For individuals with an identified address, Staples will be mailing notification letters in substantially the same form as the enclosed letter. For individuals with an unidentified address, but identified email addresses, Staples will be sending email notification in substantially the same form as the enclosed letter. In addition, Staples is providing notification on its website and by issuing a press release to major statewide media. *See* Iowa Code § 715C.2(4)(c).

Notification is being provided without unreasonable delay pursuant to the investigation described above, which was necessary to determine the nature and scope of the incident; restore the reasonable integrity, security, and confidentiality of the data system; and identify the individuals potentially affected to the extent possible. *See* Iowa Code § 715C.2(1).

Since stopping the attack, Staples has taken steps to enhance the security of its point-of-sale systems, including the use of new encryption tools. Additionally, Staples continues to cooperate with law enforcement's ongoing investigation to identify the perpetrator(s).

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Theodore J. Kobus III

Enclosures

Iowa Individual Letter

[LETTERHEAD]

[DATE]

First Name, Last Name
Address Line
Address Line 2
City, State, Zip Code

Dear Staples Customer:

We are writing to notify you of a data security incident that may have involved your payment card data from purchases that you made at a Staples store. Staples is committed to protecting your data and regrets any inconvenience caused by this incident.

Staples' data security experts detected that criminals deployed malicious software, or "malware," to some point-of-sale systems at 115 of its more than 1,400 U.S. retail stores. Staples believes that malware may have allowed unauthorized 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. 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. Staples found no malware or suspicious activity related to the payment systems at those stores. Visit http://staples.newshq.businesswire.com/statement for a complete list of affected stores and relevant dates.

Upon detection, Staples immediately eradicated the malware and further enhanced its security. Staples also retained outside data security experts to investigate the incident and worked closely with the payment card companies and law enforcement. Staples has taken steps to enhance the security of its point-of-sale systems, including the use of new encryption tools.

Staples has set up a toll-free call center, with operators standing by to address your 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 (8:00 a.m. to 8:00 p.m. CST); Saturday and Sunday: from 11:00 a.m. to 8:00 p.m. EST (10:00 a.m. to 7:00 p.m. CST).

As part of Staples' commitment to customers, Staples is offering free identity protection services from Experian, including credit monitoring, for one year to any individuals who used a payment card at any of the affected stores during the specified time periods. Details of these services are available at www.protectmyid.com/staples. 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. However, Staples will never ask for your personal information in an email. If you have any questions about the authenticity of a communication that appears to come from Staples, please call the toll-free call center at the number above.

As a precaution, you should review your account statements for any suspicious activity. If you believe your payment card may have been used for unauthorized charges, you should immediately contact your bank or payment card issuer. 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, you should promptly

report the incident to law enforcement or your state's Attorney General. If you find that your information has been misused, the Federal Trade Commission (FTC) encourages you to file a complaint with the Commission and to take these additional steps: (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.

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, regardless of whether you suspect unauthorized activity on your account. 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 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.

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. You may contact the credit reporting bureaus 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

You also can ask the credit reporting bureaus to place a "security freeze" on your credit report that prohibits them from releasing information from your credit report without your prior written authorization. For more guidance about how you can prevent, respond to, or report identity theft, you may contact local police, or the FTC or your state Attorney General at:

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

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

Sincerely,

Christine Komola
Chief Financial Officer