BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

October 31, 2013

Via UPS

Office of the New Hampshire Attorney General
Consumer Protection and Anti-Trust Bureau
33 Capitol Street
Concord, NH 03301

Attention: James Boffetti, Bureau Chief

Re: Incident Notification

Dear Mr. Boffetti:

Our client, Harbor Freight Tools USA, Inc. ("HFT"), recognizes the importance of the privacy and confidentiality of the personal information provided by its current and prospective customers. Regrettably, over the summer, Harbor Freight Tools' payment processing system was illegally attacked by cyber-criminals. The attack was similar to attacks reported by other national retailers. In response, HFT immediately engaged a leading cyber-security company to investigate and notices were posted in every store and on its website on July 20, 2013. The incident was covered by media and HFT responded to their inquiries.

Since that time, we have been working with the Payment Card Industry Forensic Investigator, HFT's payment processor, and the card associations so that the card associations can issue alerts to the banks that issued cards that may have been affected by the attack. HFT blocked the attack and adopted enhanced security measures to make its systems more secure than ever.

This incident was limited to credit and debit card transactions made in HFT's stores during a relatively short seven week period (May 6, 2013 to June 30, 2013). Transactions after June 30, 2013 were not affected. For nearly all of these transactions, HFT believes that the attacker only found "track 2" data—information on the card's

magnetic stripe that contains only the card account number, expiration date, and card verification number (track 2 does not contain the cardholder's name). For less than 1% of these transactions, the attacker may have found data that also included the cardholder's name (track 1).

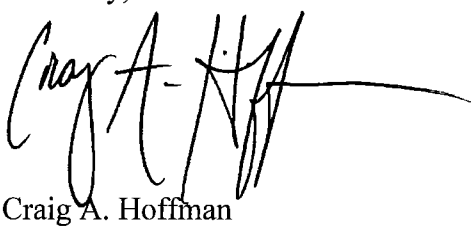
Although HFT found and blocked the attack in July, the investigation by the cyber-security company has just concluded. The nature of the attack, the type of data at risk, and the available forensic findings required extensive efforts to attempt to identify the potentially affected individuals. Because HFT could not identify any specific card that was taken or what information from that card was taken, HFT worked to identify those customers who used their cards during the impacted window for the store the card was used at. For a majority of those transactions, HFT was not able to match a name and address to the card number that was used.

Because nearly all of the transactions that were subject to unauthorized access would have only included a card number but no name, the information that could have been accessed does not meet the definition of "personal information" under N.H. Rev. Stat. § 359-C:19(IV)(a) and, thus, the statutory notification requirement would not apply. Nevertheless, HFT is mailing letters to those individuals for whom HFT had a name and address and sending an e-mail with the content of the notification letter to those individuals for whom only an e-mail was associated with the transaction. HFT has posted the contents of its notification letter on its website and issued a press release to nationwide media outlets. HFT also continues to provide a dedicated call center for affected individuals to call with questions regarding the incident.

In order to present something like this from happening in the future, HFT has conducted an internal review of its practices and procedures and is taking steps to enhance its security measures.

HFT is notifying approximately 13 New Hampshire residents by mail. Commencing today, notification is being sent to those residents in substantially the form attached hereto. Please do not hesitate to contact me if you have any questions.

Sincerely,



Craig A. Hoffman

Enclosure

HARBOR FREIGHT TOOLS®

Quality Tools at Ridiculously Low Prices

October 31, 2013

##95427-LV1-0123456 T-0012 **********5-DIGIT 12345
SAMPLE A SAMPLE
APT. 1A
123 MAIN STREET
ANYTOWN, US 99999-9999

Dear Sample A Sample:

Over the summer, Harbor Freight Tools' payment processing system was illegally attacked by cyber-criminals. The attack was similar to attacks reported by other national retailers. In response, we immediately engaged a leading cyber-security company to investigate and notices were posted in every store and on our website. We blocked the attack and adopted enhanced security measures to make our systems more secure than ever.

Fortunately, this incident was limited to credit and debit card transactions made in our stores during a relatively short seven week period (May 6, 2013 to June 30, 2013). Transactions after June 30, 2013 were not affected. For nearly all of these transactions, we believe that the attacker only found "track 2" data—information on the card's magnetic stripe that contains only the card account number, expiration date, and card verification number. For less than 1% of these transactions, the attacker may have found data that also included the cardholder's name.

Because we cannot identify which specific cards or information were actually taken, we are notifying our customers that we have been able to identify whose cards were used during the May 6, 2013 to June 30, 2013 time frame at each impacted store. We believe your card was in this group.

If you see a fraudulent charge on your card, please immediately contact the bank that issued your card. Major credit card companies typically guarantee cardholders will not be responsible for fraudulent charges. Please be on the lookout and review your account statements for any unauthorized activity. We have included additional information about ways you can protect yourself on the back of this letter.

We regret any inconvenience this may cause. Keeping customer information secure is a top priority at Harbor Freight and we will continue to work to make our network more secure. If you have questions, please call us toll free at 877-216-4023, Monday through Friday, 9 a.m. – 7 p.m. EST, and use the following ten digit reference number when calling: 4471100813.

Sincerely,

Eric Smidt
President, Harbor Freight Tools

More Information on Ways to Protect Yourself

We recommend that you remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 6790, Fullerton, CA 92834, www.transunion.com, 1-800-680-7289

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the attorney general's office in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.