EDWARDS WILDMAN

EDWARDS WILDMAN PALMER LLP
225 WEST WACKER DRIVE, SUITE 3000
CHICAGO, IL 60606
+1 312 201 2000 main +1 312 201 2555 fax
edwardswildman.com

Thomas J. Smedinghoff
Partner
+1 312 201 2021
fax +1 855 593 0972
tsmedinghoff@edwardswildman.com

August 27, 2013

VIA FEDERAL EXPRESS

Attorney General Joseph Foster
New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Midwest Supplies, LLC
Notification of Security Breach Pursuant to N.H. Rev. Stat. § 359-C.20

Dear Attorney General Foster:

We write to advise you of a data security incident involving potential unauthorized access to personal information of New Hampshire residents. The incident involved malware inserted on a webserver used to host the website of our client, Midwest Supplies, LLC, located in St. Louis Park, Minnesota (the "Company").

Learning about and responding to the Incident. The Company first received preliminary information regarding a potential security incident on July 19, 2013. Thereafter, the Company immediately: (i) investigated the matter, and identified, located and removed malware apparently causing the problem, (ii) retained a third party forensic firm to investigate the incident to determine the extent of any unauthorized access or acquisition; (iii) engaged our law firm to oversee forensics, coordinate appropriate data breach response, provide advice regarding legal obligations pursuant to applicable law, and notify law enforcement as appropriate; (iv) ensured that its credit card processor, the sponsoring bank, and the credit card brands were notified; and (v) committed to notify affected individuals.

The forensic investigation, which was substantially completed on or about August 22, 2013, revealed that this incident involved malware inserted on the Company's server supporting Internet sales transactions, which malware appears to have been used to capture and email customer information to an unauthorized third party. The information potentially exposed includes customer names, addresses, email addresses, telephone numbers, credit card numbers, and credit card expiration dates and security codes. The malware has been removed and the Company believes that the server is now secure. The Company does not store credit card information.

EDWARDS
WILDMAN

The forensic investigation determined that credit card transactions processed on the Company's website between June 13, 2013 and July 19, 2013 were at high risk of compromise. Based upon records of sales transactions for that time period, the Company determined that 29 New Hampshire residents were potentially affected by this incident. In addition, the forensic investigation was not able to rule out the possibility that certain credit card transactions processed on the Company's website between February 27, 2013 and June 13, 2013 could potentially have been compromised, although it did not find conclusive evidence regarding compromise of such transactions. In an abundance of caution, the Company is notifying the additional 93 potentially affected New Hampshire residents whose information could potentially have been compromised between February 27, 2013 and June 13, 2013.

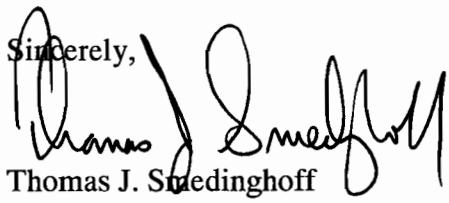
Communicating with Affected Individuals. The Company has arranged with a third party mailing firm to send letters to the affected individuals notifying them of this incident. The applicable data has been sent to the mailing firm, and based on its processing lead time requirements we expect that such notification letters will be sent out to the affected individuals by First Class Mail on or about August 31, 2013. A template of the notification materials is enclosed with this letter.

Efforts to Deter Future Breach. The Company has taken several important steps to improve the level of its data security following this incident, including implementing certain technical security enhancement measures, changes in security policies, and increasing the profile of data security issues within the organization at all levels.

* * * * *

We trust that this letter and its enclosure provide you with the information required to assess this incident and the Company's response. Please let us know if you have any questions or if we may be of further assistance.

Sincerely,



Thomas J. Smedinghoff

Enclosure

cc: David Kidd, President, Midwest Supplies, LLC

Midwest Supplies, LLC - 1955 County Rd C2 W - Roseville, MN 55113

August 31, 2013

[Recipient]
[Address 1]
[Address 2]
[City] [State] [Zip]

Regarding your credit card account(s):
[Last 4 digits of card number]

Dear Fellow Homebrewer.

We're writing to tell you that it's possible that the credit card you used at Midwest Supplies on [Month, Day, Year] might have been compromised at that time. Despite our best efforts, the security of our website was breached by an outside party. Your credit card information might have been improperly viewed including your name, address, email address, telephone number, credit card number, expiration date and security code.

As soon as we discovered the breach, we took immediate measures to resolve the situation and are satisfied that it is, in fact, resolved. We conducted a full investigation and have taken extensive steps to prevent it from happening again.

You should carefully monitor your monthly credit card statements for unusual charges. Be advised that if you see charges that you believe are suspect, you should immediately contact your credit card company directly. For additional information about how to protect yourself in situations such as these, please see the other side of this letter.

We know that this situation is inconvenient and creates unnecessary worry and concern. Feel free to call us directly at 1-888-449-2739 if you have any questions.

In the meantime we'd like to offer you our sincere apologies. We take privacy and security very seriously.

We've spent many years working to earn your trust and loyalty. And we recognize that an attack on us like this can undermine that trust. As one homebrewer to another, you can rest assured that we won't rest until you've brewed your best. Let's help you do just that ... please accept this $25 coupon, reference code [SY-XXXXXX] as a gesture of apology for the inconvenience you might have experienced.

David Kidd
President

Additional Information and U.S. State Notification Requirements

There are a number of steps you should consider to guard against identity theft.

Review Your Account Statements and Credit Report: It is recommended that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports. Report any fraudulent transactions to the creditor or credit reporting agency from whom you received the statement or report. You may obtain a free copy of your credit report from each credit reporting agency once every 12 months, whether or not you suspect any unauthorized activity on your account, by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form available at that website and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report at any time by contacting any one or more of the national credit reporting agencies listed below.

Equifax	Experian	TransUnion (FVAD)
P.O. Box 740241	P.O. Box 2002	P.O. Box 105281
Atlanta, Georgia 30374	Allen, TX 75013	Atlanta, GA 30348-5281
www.equifax.com	www.experian.com	www.transunion.com
1-800-685-1111 Credit Reports	1-888-397-3742 Credit Reports	1-800-888-4213 Credit Reports
1-888-766-0008 Fraud Alert	1-888-397-3742 Fraud Alert	1-800-680-7289 Fraud Alert
1-800-685-1111 Security Freeze	1-888-397-3742 Security Freeze	1-800-680-7289 Security Freeze

Federal Trade Commission and State Resources: General guidance on protecting yourself from identify theft is available from the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington D.C. 20580, by phone at 877-ID-THEFT (438-4338), and/or from the FTC website at http://www.ftc.gov/bcp/edu/microsites/idtheft. In many states, additional information is also available from your state's Attorney General's Office.

Fraud Alerts and Security Freezes: You may obtain information about fraud alerts and security freezes (also referred to as credit freezes), including how to place a fraud alert or security freeze, from the Federal Trade Commission or credit reporting agencies at the contact information provided above. However, be aware that a fraud alert or security freeze may interfere with or delay legitimate requests for credit approval.

For residents of Iowa:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:
State law advises you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Maryland and North Carolina:
You can obtain information from the Maryland and North Carolina Offices of the Attorney General about steps you can take to avoid identity theft.

Maryland Office of the Attorney General	North Carolina Office of the Attorney General
Consumer Protection Division	Consumer Protection Division
200 St. Paul Place	9001 Mail Service Center
Baltimore, MD 21202	Raleigh, NC 27699-9001
1-888-743-0023	1-877-566-7226
www.oag.state.md.us	www.ncdoj.com