



Bushnell Law

CHRISTOPHER L. HARLAN, Licensed in ID & MT • BRANDON D. HAJNY, Licensed in ID, CO, NM & TX
THOMAS A. BUSHNELL, Licensed in ID, WA & CA

BUSHNELL LAW
6430 Kootenai Street
PO Box 1833 (mailing address)
Bonners Ferry, ID 83805
Tom@Bushnell.Law
Chris@Bushnell.Law
Brandon@Bushnell.Law
www.Bushnell.Law
Phone: (208) 267-9321
Fax: (208) 946-5714

September 25, 2024

Consumer Protection Division Office

44 North Potomac Street
Suite 104
Hagerstown, MD 21740

Notification of Breach: Northwest Crop Protection



To whom it may concern,

Our office has been retained by Northwest Crop Protection for the limited scope of providing notification of the recently discovered breach of said company's website. Despite best efforts of our client, actual knowledge of the occurrences is severely limited, and forensics conducted by an external digital forensics firm, Net Guardians, now defunct, was nonconclusive.

What Happened

According to the limited knowledge we were able to gather, the company website infrastructure was breached in during the first quarter of 2023, which resulted in customer credit card and billing information being stolen, and in some cases, used in fraudulent purchases. It was through these purchases that Northwest Crop Protection was made aware of a potential breach.

According to the initial findings by Net Guardians, the breach likely originated from a suspicious file located in a shared Dropbox account that was connected to the website host network. It was additionally found that the original hosting platform was no longer secure, or otherwise did not meet web hosting standards on levels of security, which included failing to encrypt the database which stored the customer billing information. Credit card numbers, expiration dates, and card security codes were not stored on the host server and were immediately transferred to the Authorize.net payment processor API after being entered into the website for payments. It is not known how the credit card information specifically was obtained by the unauthorized individuals.

Steps Taken

At the request of Net Guardians, Northwest Crop Protection rebuilt their webhost and infrastructure from the ground up to ensure it complied with commercial security practices, including the usage of hardened hosting, two factor authentication for all server administration

actions, and installing Managed Endpoint Detection and Response (mEDR) software on all servers and user computers. Northwest Crop Protection has complied with all requests for additional information from agencies but is unaware if any further action by law enforcement was taken against the unauthorized users.

Affected Individuals In Your State

Northwest Crop Protection has identified that 142 residents within Maryland were possibly affected as a result of this breach, and notification was sent to all affected users through the email the users utilized when signing up for the site. In matters of bounce-back or undeliverable email, a physical letter was sent to the billing address on file instead. A generic copy of the letter sent to affected individuals in your state is provided along with this letter.

Thank you,

A handwritten signature in black ink, appearing to read 'CH' followed by a stylized flourish.

Christopher Harlan
Bushnell Law

Keystone Pest Solutions LLC
Online Store for Northwest Crop Protection LLC
205 Day Break Rd
Bonners Ferry, ID 83805

[DATE]

Notice of Data Breach

Dear Customer:

We are contacting you to notify you of a security breach that occurred at Keystone Pest Solutions LLC. As one of our valued customers, it is our responsibility to notify you and provide you with the necessary information to protect yourself.

What Happened:

We recently discovered that our system had been accessed by an unauthorized individual or group during the first quarter of 2023. This breach resulted in the potential exposure of personal information related to credit cards used to purchase through our payment processor, including credit card numbers and billing information.

What Information Was Involved:

The incident involved your credit card information, more specifically: credit card numbers, types, expiration dates, and CVV numbers, and their associated names and billing addresses tied to those cards as entered into the site.

What We Are Doing:

As soon as we became aware of the breach, we took immediate action to investigate the incident and secure our systems. We engaged a professional team dealing in cybersecurity breaches to assist us in identifying the extent of the breach and implementing additional security measures to prevent future incidents. This has resulted in a complete overhaul of our backend systems with increased security to ensure a similar breach does not repeat in the future.

What You Can Do:

We recommend that you take the following steps to protect yourself from any potential misuse of your personal information:

1. **Monitor your financial accounts**, credit reports, and any other relevant accounts for any suspicious activity.
2. **Consider placing a fraud alert or credit freeze on your credit reports** to prevent unauthorized access to your credit information. The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. This fraud alert tells creditors to contact you before any new accounts are opened in your name or changes are

made to your existing accounts. A fraud alert can be requested from any one of the three major credit bureaus, which will stay on your credit report for one (1) year.

Equifax

Phone 1-888-378-4329
Address Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348-5788
Web Links Home Page:
<https://www.equifax.com>
Credit Report:
<https://www.equifax.com/personal/credit-report-services/free-credit-reports/>
Security Freeze:
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
Fraud Alert:
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Experian

Phone 1-888-397-3742
Address Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
Web Links Home Page:
<https://www.experian.com>
Credit Report:
<https://www.experian.com/consumer-products/free-credit-report.html>
Security Freeze:
<https://www.experian.com/freeze/center.html>
Fraud Alert:
<https://www.experian.com/fraud/center.html>

TransUnion

Phone 1-800-888-4213
Address TransUnion
P.O. Box 160
Woodlyn, PA 19094
Web Links Home Page:
<https://www.transunion.com>
Credit Report:
<https://www.transunion.com/get-credit-report>
Security Freeze:
<https://www.transunion.com/credit-freeze>
Fraud Alert:
<https://www.transunion.com/fraud-alerts>

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at <https://www.identitytheft.gov/> to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also consider placing a free credit freeze, which will prevent potential creditors from getting your credit report. This makes it less likely for identity thieves to open new accounts in your name. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

3. **Report any suspected identity theft or fraudulent activity** to the appropriate authorities, including your local law enforcement, attorney general's office, and the Federal Trade Commission.

Federal Trade Commission

Phone 1-877-382-4357
Address Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Web Links Home Page:
<https://www.ftc.gov>
Identity Theft Reporting:
<https://www.identitytheft.gov/#/>

Attorney General for Maryland

Phone 410-576-6300
Address Consumer Protection Division Office
44 North Potomac Street
Suite 104
Hagerstown, MD 21740
Web Links Home Page:
<https://www.marylandattorneygeneral.gov/>

4. **Change passwords for your online accounts**, especially if the same password is used for multiple accounts. If you do not already use a password manager, consider trying one of these free options:

Standalone Applications (with free Personal Plans)

Bitwarden <https://bitwarden.com/products/personal/>
Dashlane <https://www.dashlane.com/personal-password-manager>
KeePass <https://keepass.info>
LastPass <https://lastpass.com/create-account.php>

Free Browser or Operating System Solutions

Google Chrome Android, iOS, Linux, MacOS, Windows
<https://passwords.google.com>
iCloud Keychain / Apple Passwords iOS, MacOS
<https://support.apple.com/en-us/109016>
Microsoft Edge Android, iOS, Linux, MacOS, Windows
<https://support.microsoft.com/en-us/microsoft-edge/save-or-forget-passwords-in-microsoft-edge-b4beecb0-f2a8-1ca0-f26f-9ec247a3f336>

Mozilla Firefox

Android, iOS, Linux, MacOS, Windows

<https://support.mozilla.org/en-US/kb/password-manager-remember-delete-edit-logins>

5. Be cautious of phishing attempts or suspicious emails, calls, or texts asking for personal or financial information.

For More Information:

If you have any questions or concerns regarding this data breach, please do not hesitate to contact our dedicated customer support team at (208) 297-3595 or support@keystonepestsolutions.com.

We deeply regret any inconvenience or concern this incident may have caused you. We take the security of your personal information very seriously and will continue to enhance our security measures to prevent such incidents in the future.

Thank you for your understanding and ongoing support.

Sincerely,

Wes Weaver

President

Northwest Crop Protection LLC