

STATE OF NH
DEPT OF JUSTICE

2021 JAN 25 PM 1:27

BakerHostetler

Baker & Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Benjamin D. Wanger
direct dial: 215.564.1601
bwanger@bakerlaw.com

January 22, 2021

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

I am writing to notify you of a data security incident on behalf of my client, Master Halco, Inc., a manufacturer and wholesale distributor of perimeter security and fencing located in Fairfield, Ohio.

Master Halco recently concluded an investigation concerning an email phishing campaign that targeted some of its employees. Upon learning of the incident, Master Halco promptly secured the employees' email accounts and launched an investigation. A third-party cybersecurity forensics firm was engaged to assist.

In connection with that investigation, Master Halco learned that an unauthorized party gained access to several employees' email accounts at various times between September 2, 2020 and September 14, 2020. Master Halco's investigation was unable to determine whether the unauthorized party actually viewed any emails or attachments in the accounts. In an abundance of caution, Master Halco reviewed the emails and attachments contained in the email accounts to identify individuals whose information may have been accessible to the unauthorized party. On December 30, 2020, Master Halco determined that the personal information of two New Hampshire residents were in the account and included the individuals' name and one or more of the following: Social Security number, driver's license number, financial account number and/or payment card number.

January 22, 2021

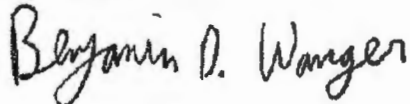
Page 2

On January 22, 2021 Master Halco will mail notification letters via U.S. mail to the New Hampshire residents whose personal information may have been involved in this incident.¹ Master Halco is offering residents with affected Social Security or driver's license numbers one year of complimentary credit monitoring and identity theft protection service through Experian. Master Halco is also providing a dedicated call center for individuals to call with any questions regarding the incident.

To help prevent a similar incident from occurring in the future, Master Halco has implemented additional security measures to enhance the security of our network and retrained our employees concerning data security.

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

Sincerely,

A handwritten signature in black ink that reads "Benjamin D. Wanger". The signature is written in a cursive style with a large initial 'B'.

Benjamin D. Wanger
Counsel

Enclosure

¹ This notice is not, and does not constitute, a waiver of Master Halco's objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this data security incident.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

Dear <<Name 1>>:

Master Halco, Inc. understands the importance of protecting the privacy and security of the information we maintain. We are writing to inform you about a data security incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

Master Halco recently concluded an investigation concerning an email phishing campaign that targeted some of our employees. Upon learning of the incident, we promptly secured the employees' email accounts and launched an investigation. A third-party cybersecurity forensics firm was engaged to assist.

In connection with that investigation, we learned that an unauthorized party gained access to several employees' email accounts at various times between September 2, 2020 and September 14, 2020. Our investigation was unable to determine whether the unauthorized party actually viewed any emails or attachments in the accounts. In an abundance of caution, we reviewed the emails and attachments contained in the email accounts to identify individuals whose information may have been accessible to the unauthorized party. On December 30, 2020, we determined that the accounts included an email and/or attachment containing your <<VARIABLE DATA>>

To date, we are unaware of any misuse of the information maintained in the employees' email accounts, nor do we have any evidence that any emails or attachments containing your information were actually viewed. However, we want to inform you of this event and provide you with information about how you can protect your information. As a precaution, we have secured the services of Experian® to offer you a complimentary one-year membership in Experian's IdentityWorksSM. This product helps detect possible misuse of your credit information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect your information, please see the pages that follow this letter.** We also encourage you to remain vigilant by regularly reviewing your financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institution immediately.

To help prevent a similar incident from occurring in the future, we have implemented additional security measures to enhance the security of our network and retrained our employees concerning data security. If you have any questions, please call our dedicated call center at 800-377-2214 Monday through Friday from 9 am to 9 pm Eastern Time.

Sincerely,

A handwritten signature in black ink, consisting of a stylized 'S' followed by a series of loops and a final upward stroke.

Sergio Narikawa
Chief Financial Officer and Chief Compliance Officer

EXPERIAN CREDIT MONITORING ENROLLMENT INSTRUCTIONS

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<Activation Code>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.288.8057. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877.288.8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877.288.8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdiction

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free 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 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. 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. Contact information for the Federal Trade Commission is as follows:

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

You can contact Master Halco, Inc. via U.S. mail at 3010 Lyndon B Johnson Fwy, Suite 800, Dallas, TX 75234 or via phone at 800-883-8384.

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.