Moss & Barnett

March 31, 2021

VIA E-MAIL

Office of the New Hampshire Attorney General
DOJ-CPB@doj.nh.gov

Re: The Walman Optical Company Data Breach Notification

To the Office of the New Hampshire Attorney General:

This law firm represents The Walman Optical Company ("Walman"). I write to inform you of a data security incident involving Walman. On August 21, 2020, Walman learned that an unauthorized party gained access to Walman's computer network and infiltrated data from one of its servers through a ransomware attack. Walman immediately initiated an investigation and retained a leading computer security firm to stop the attack and restore the computer systems to normal operations, as well as retained an independent cyber forensic company to analyze the information that was accessed. Walman also cooperated with the FBI as they investigated the group that conducted the attack.

During the course of the investigation, neither the FBI investigation nor the cyber forensics analysis discovered that personal information was actually accessed as part of this attack, however the information was accessible. The personal information that was accessible includes Walman employees' and former employees' name, address, Social Security number, date of birth, and in some cases wage and ESOP account value information. There are three (3) residents of the state of New Hampshire whose information was accessible on this server.

As a result of this incident, Walman has implemented several security improvements to strengthen its network and data security. Walman has also arranged to provide credit monitoring and identity protection services to affected individuals. More information regarding this incident is described in the attached sample notification letter. The notification letter was sent directly to the affected residents on March 19, 2021.

Please contact me with any questions or concerns.

Thank you,

/s/ Brianna Blazek

Brianna Blazek
Attorney at Law
P: (612) 877-5277 F: (612) 877-5057
Brianna.Blazek@lawmoss.com

6861697v2

WALMAN

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?
On August 21, 2020, Walman's computer systems experienced a ransomware attack. The apparent purpose of the attack was to damage Walman's computer systems and download valuable information. In response to the attack Walman engaged ESX, a respected security company, to work with us to stop the attack and restore our computer systems to normal operations. Walman also cooperated with the FBI as they investigated the group that conducted the attack. During the course of their investigation, the FBI discovered that information from a Walman server had been downloaded and posted on the Internet. Further investigation indicated that the information was downloaded from a single server on Walman's network. Walman engaged an independent cyber forensics company to analyze the information on this server. The analysis concluded that your personal information was stored on this server and was unprotected during the attack. No indication has been found that your personal information was accessed or downloaded. Out of an abundance of caution, Walman is notifying you that your personal information may have been exposed.

You may wonder why we are contacting you now. It has taken some time to complete the investigation and conduct the forensic analysis. After reviewing the investigation results, Walman decided to notify you about this security incident even though there is no indication that your personal data was accessed or downloaded.

What information was involved?
Your personal information including **name, address, Social Security number, date of birth, and compensation and retirement information** may have been exposed.

What we are doing.
Walman has implemented several security improvements to strengthen our network and data security. In addition, we have changed the way we store personal information to reduce potential exposure.

To help you be more secure, we are offering identity monitoring services for one year from Kroll, a global leader in risk mitigation and response. **Information accompanies this notification letter that describes the services Walman is offering to you.**

In addition, a dedicated hot line has been established at 1-855-660-1528. You can call to get more information or assistance activating the identity monitoring services being offered Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

What you can do.
Read the enclosed material from Kroll. If you have questions or need assistance activating identity monitoring services, you can call the dedicated hotline at 1-855-660-1528.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.
We take the protection and proper use of personal information very seriously. We encourage you to use the resources and services presented in this notification.

Please know that we sincerely regret any inconvenience or concern this incident may cause you.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

Activate Identity Monitoring Services:

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **June 23, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Kroll | A Division of DUFF&PHELPS

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of 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 at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

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

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.