WALMAN
OPTICAL

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

<<last_name>>
<<b2b_text_1(Attn)>>
<<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 employee's Personal Health Information (PHI). We take the protection and proper use of PHI 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 that server. The analysis determined that employee PHI (**employee name and optical prescription**) appears on safety eyewear invoices that were stored on this server. No additional PHI appears on the invoices. An unknown number of these invoices were downloaded from Walman's server. Some of the downloaded invoices were displayed on the Internet. Walman Optical believes the exposed PHI presents a very low risk to you and your employees. Out of an abundance of caution, Walman is notifying you that PHI associated with the invoice numbers listed below 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. Since Walman does not have contact information for the employees associated with the invoices listed below, we are notifying you of the potential exposure of your employee's PHI.

What information was involved?
PHI (**employee name and optical prescription**) as it appears on each Walman Optical safety eyewear invoice listed below. The listed invoices were dated between May 1st and July 31st. No additional PHI appears on the invoices. An unknown number of these invoices were downloaded from Walman's server. Some of the downloaded invoices were displayed on the Internet.

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 PHI to reduce potential exposure.

A Frequently Asked Questions web page with more information about this security incident is available for you and your employees at: **www.walman.com/2020hipaanotify**

In addition, a dedicated hot line has been established for you or your employees at 1-855-660-1528. Assistance is available Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

What you can do.
You may choose to notify the employees associated with the invoice numbers listed below about this security incident. You may also choose to share the Frequently Asked Questions web page (**www.walman.com/2020hipaanotify**), dedicated hotline (1-855-660-1528) and the attached Additional Resources page.

For more information.
We take the protection and proper use of PHI very seriously. Walman Optical believes that the PHI (**employee name and optical prescription**) that was potentially exposed presents a very low risk to you and your employees. We encourage you and your employees to visit the Frequently Asked Questions web page and call the Hotline for more information.

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

IMPACTED INVOICES

<<b2b_text_2(ImpactedInvoices)>><<b2b_text_3(ImpactedInvoices2)>><<b2b_text_4(ImpactedInvoices3)>><<b2b_text_5(ImpactedInvoices4)>><<b2b_text_6(ImpactedInvoices5)>>

ADDITIONAL RESOURCES

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.