

October 4, 2022

Robert Walker
601.499.8083 (direct)
601.499.8077 (main)
Robert.Walker@WilsonElser.com

Via Electronic Mail

Attorney General Brian Frosh
Office of the Attorney General
Attn: Security Incident Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: Cybersecurity Incident Goodwill Industries of New Mexico
Wilson Elser File # : 16516. 01932

Dear Attorney General Frosh:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Goodwill Industries of New Mexico (“GINM”) with respect to a recent data privacy incident (hereinafter, the “Incident”). GINM takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that GINM has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of Incident

On August 17, 2022, GINM discovered it was subject of a cyber attack when its employee was unable to log into his business email account. It was then determined that the Exchange server, along with the file server, was down. Upon discovery of the attack, GINM moved quickly to initiate a response, which included shutting down and securing the network. GINM also engaged a specialized third-party cybersecurity firm to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. On August 31, 2022, GINM discovered that information related to current and former employees was potentially compromised. On September 12, 2022, GINM determined that information pertaining to some of its customers was also potentially compromised.

Although GINM is unaware of any fraudulent misuse of information, the following data elements may have been exposed as a result of the unauthorized activity: first name, last name, address, social security number, date of birth, and phone number. Out of an abundance of caution, GINM is reporting the Incident and notifying potentially affected individuals.

As of this writing, GINM has not received any reports of related identity theft since the date of the Incident.

2. Number of Maryland residents affected.

A total of four (4) Maryland residents have been potentially affected by this incident. Notification letters to individuals were mailed to potentially impacted individuals on September 20 and October 3, 2022, by first class mail. A sample copy of the notification letter is included with this letter under *Exhibit A*.

3. Steps taken in response to the Incident.

GINM is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, GINM moved quickly to respond to the Incident, ensured the security of its systems moving forward, and notified the potentially affected individuals.

Although GINM is not aware of any actual or attempted misuse of the affected personal information, GINM offered complimentary credit monitoring and identity theft restoration services through a third party vendor to all potentially affected individuals. Additionally, GINM provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

GINM remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Robert.Walker@WilsonElser.com or 601-499-8083.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

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

Robert Walker, Esq.

RW/ejl

Exhibit A

Goodwill Industries of New Mexico
<<Return Address>>
<<City>>, <<State>> <<Zip Code>>

To Enroll, Please Call:
1-833-875-0572
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Via First-Class Mail

October 3, 2022

Dear <<First Name>> <<Last Name>>:

The purpose of this letter is to inform you of an incident that may have exposed your personal information. We take the security of your private data seriously and apologize for any inconvenience or concern this may cause. However, as you will see in the following description, we detected the attack very early and we were able to shut down our systems and mitigate the situation quickly.

What Happened and What Information was Involved:

On August 17, 2022, a Goodwill Industries of New Mexico ("GINM") employee was unable to log into his business email account and then determined that the Exchange server was down. It was determined that the file server was also down, and GINM's network was the victim of a cyber-attack. Upon discovery of the attack, we moved quickly to initiate a response, which included shutting down and securing the network. We quickly engaged a team of cyber security professionals to conduct a forensic investigation to fully determine the scope and the overall impact of the incident.

After a thorough review of the files potentially accessed by the unauthorized third party, GINM has determined that the following personal information of yours could have been accessed: first name, last name, address, social security number, date of birth, and phone number.

While we have no evidence that any of your personal information was compromised or misused in any manner, we are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.

What We Are Doing:

Data security is one of our highest priorities. We value the safety of your personal information. GINM has made immediate enhancements to our systems, security and practices. Additionally, we have engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that enhanced security protocols are in place going forward. We are committed to helping those people who may have been impacted by this unfortunate situation.

In response to the incident, although there is no evidence that your information has been misused for the purpose of committing fraud or identity theft, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-875-0572 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX

representatives are available Monday through Friday from 7 am - 7 pm Mountain Time. Please note the deadline to enroll is January 3, 2023.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-875-0572 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

Shauna Kastle
President/CEO

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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 five 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police

report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

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, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.