

January 4, 2021

Ryan M. Cook
601.499.8087 (direct)
Ryan.Cook@wilsonelser.com

Via electronic-mail: Idtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re:	Our Client	:	Toledo Lucas County Public Library
	Matter	:	Data Security Incident on October 31, 2021
	Wilson Elser File #	:	16516.01674

Dear Attorney General Frosh:

We represent Toledo Lucas County Public Library (“TLCPL”), located in Toledo, Ohio, with respect to a potential data security incident described in more detail below. TLCPL takes the security and privacy of the information in its control 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 security breach, what information has been compromised, and the steps that TLCPL is taking to restore the integrity of the system. We have also enclosed hereto a sample of the notification made to the potentially impact individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On or around October 31, 2021, TLCPL was the target of a cybersecurity incident. An unauthorized third party attempted to infiltrate TLCPL’s computer systems. This incident may have resulted in the exposure of personal information that is located on TLCPL’s systems, including names, social security numbers, and dates of birth.

TLCPL, however, is not aware of any evidence that information has been misused. TLCPL has not received any reports of related identity theft since the date of the incident (October 31, 2021 to present).

2. Number of Maryland Residents Affected

A total of three (3) residents of Maryland were potentially affected by this security incident. Notification letters to these individuals were mailed on December 30, 2021, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Upon learning of this incident, TLCPL moved quickly to institute a response plan, which included conducting an investigation with the assistance of third-party forensic specialists and engaging in steps to confirm the security of any relevant systems. TLCPL has reported this incident to law enforcement. TLCPL has reviewed, altered and enhanced its policies and procedures relating to the security of its systems and servers, as well as its information life cycle management.

4. Contact Information

TLCPL is committed to the protection and security of its sensitive information. If you have any questions or need additional information, please do not hesitate to contact me at Ryan.Cook@WilsonElser.com or (601) 499-8087.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

A handwritten signature in black ink, appearing to read "Ryan Cook", written in a cursive style.

Ryan M. Cook, Esq.

Enclosure: *Sample Notification Letter*

Toledo Lucas County Public Library

<<Return Address>>

<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>

<<Address1>> <<Address2>>

<<City>>, <<State>> <<Zip>>

Via First-Class Mail

December 30, 2021

Notice of Data Incident

Dear <<First Name>> <<Last Name>>,

We are writing in order to inform you of an incident resulting in the exposure of your sensitive personal information to an unauthorized actor. While we cannot be sure that your data will be misused, our extensive internal review has confirmed that your data was accessible during the compromise. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

What Happened:

On October 31, 2021, Toledo Lucas County Public Library was the subject of a sophisticated cyber attack against its network. An unauthorized party gained access to our network environment and encrypted our data. Our IT professionals immediately secured the network upon discovery of the compromise. We then retained professional, independent forensic experts to investigate the extent of the unauthorized activity and to ensure that our environment was secure.

Our investigation has determined that your employee information was located in a file on the compromised system, including <<variable text 1>>. This information was stored on our system as part of our standing employment practices, namely payroll, human resources, and onboarding.

As of this writing, we have not received any reports of related identity theft since the date the incident was discovered (October 31, 2021), however we recommend following the steps listed below to protect your data from any potential misuse.

What We Are Doing:

We have ensured that no further unauthorized activity has continued. We have reviewed and altered our policies and procedures relating to the security of our systems and servers. We continue to remain committed to systems security, data privacy, and the protection of your personal information.

We value the safety of your personal information and are therefore offering credit monitoring and identity theft protection services through IDX, a leading identity protection technology company. IDX's services include: <<12 / 24>> months of credit monitoring 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 free identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday, 9 am – 9 pm Eastern Time. Please note the deadline to enroll is March 30, 2022.

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 sensitive 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:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call IDX at 1-800-939-4170, Monday through Friday, 9 am – 9 pm Eastern Time.

Toledo Lucas County Public Library values the security of the personal data that we protect, and we apologize for any inconvenience that this incident has caused.

Sincerely,

Toledo Lucas County Public Library

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 listed above.

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.