



October 24, 2024

Daniel Parziale

504.702.1712

Daniel.Parziale@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: Cybersecurity Event Involving Village of Skokie.

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents the Village of Skokie (“Skokie”), a municipality located in Skokie, Illinois, with respect to a recent cybersecurity event that was first discovered by Skokie on December 18, 2023 (hereinafter, the “Event”). Skokie takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar event from occurring in the future.

This letter will serve to inform you of the nature of the Event, what information may have been compromised, the number of Maryland residents being notified, and the steps that Skokie has taken in response to the Event. We have also included with this letter a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services. By providing this notice, Skokie does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

1. Nature of the Event

On December 18, 2023, Skokie detected unusual activity on its network environment. Upon discovery of this Event, Skokie immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment and conducting a comprehensive forensic investigation to determine the nature and scope of the Event. Skokie learned that an unauthorized actor acquired certain files and data stored within Skokie’s network.

Upon learning this, Skokie launched a review of the potentially affected data to identify the individuals and information involved. On September 16, 2024, Skokie identified additional persons whose sensitive information was potentially included within the impacted data.

Although Skokie is unaware of any fraudulent misuse of information, it is possible that individuals' First Name, Last Name, Date of Birth, Driver's License, and Social Security Number may have been exposed as a result of this unauthorized activity.

2. Number of Maryland residents affected.

A total of 1 Maryland resident may have been potentially affected by this Event. A notification letter was sent to the potentially impacted individual on October 24, 2024, 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 Event.

Skokie is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar Event from occurring in the future. Upon discovery of the Event, Skokie moved quickly to investigate and respond to the Event, assessed the security of its systems, and notified the potentially affected individuals. Specifically, Skokie engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Event. Additionally, Skokie installed Huntress endpoint protection; installed SentinelOne (S1) Advanced Endpoint Detection; reset all passwords, including those of domain and privileged accounts, and updated all firewalls. Lastly, Skokie informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although Skokie is not aware of any actual or attempted misuse of the affected personal information, Skokie is offering 12-24 months of complimentary credit monitoring and identity theft restoration services through TransUnion to all individuals to help protect their identity. Additionally, Skokie 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

Skokie 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 Daniel.Parziale@WilsonElser.com or 312.821.6164.

Regards,

A handwritten signature in black ink that reads "Daniel Parziale". The signature is written in a cursive, flowing style.

Wilson Elser Moskowitz Edelman & Dicker LLP

Exhibit A

Village of Skokie
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P

A large black rectangular redaction box covering the majority of the first page's content, with a small white rectangular cutout on the right side.

000010103G0500

P



Village of Skokie

October 24, 2024

Village Hall

5127 Oakton Street
Skokie, Illinois 60077

Phone (847) 673-0500
Fax (847) 673-0525

www.skokie.org
SkokieVision Municipal Cable
1660 AM Skokie

Council-Manager Government

Mayor George Van Dusen
Clerk Pramod C. Shah
Trustees James H. Johnson
Khem Khoeun
Ralph Klein
Alison Pure Slovin
Keith A. Robinson
Edie Sue Sutrer
Manager John T. Lockerby
Counsel Michael M. Lorge

Awards and Distinctions

American Public Works
Association (APWA)
Accreditation

Commission on Fire
Accreditation International
(CFAI)

Gold Level Clean Air Counts
Community

Government Finance Officers
Association Budget Award

Government Finance Officers
Association Certificate of
Achievement for Excellence in
Financial Reporting

Illinois Law Enforcement
Accreditation (ILEAP)

Insurance Services Office (ISO)
Class One Fire Department

State of Illinois Certified Health
Department

Tree City U.S.A. Distinction

Re: Notice of Data Security Event

Dear [REDACTED],

The Village of Skokie ("Skokie") is writing to inform you of a recent data security Event that may have resulted in unauthorized access to your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the Event, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On December 18, 2023, Skokie detected unusual activity on our network. Upon discovery of this Event, Skokie immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment and conducting a comprehensive forensic investigation to determine the nature and scope of the Event. The investigation revealed that an unauthorized actor has acquired certain files and data stored within Skokie's network.

Upon learning this, Skokie launched a review of the potentially affected data to identify the individuals and information involved. On September 16, 2024, Skokie identified persons whose sensitive information was potentially included within the impacted data.

What Information Was Involved?

Although Skokie has no evidence that any sensitive information has been misused by third parties as a result of this Event, we are notifying you out of an abundance of caution and for purposes of full transparency. The impacted information varied by individual. Based on the investigation, the following information may have been subject to unauthorized access: First Name, Last Name, Date of Birth, Driver's License Number, and Social Security Number.

As of this writing, we have not received any reports of related identity theft since the date of the Event (December 18, 2023, to present). We would like to reassure you that we have taken all efforts possible to mitigate any further exposure of your personal information, and we are committed to supporting you.

What We Are Doing

Data privacy and security is among Skokie's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the Event, Skokie moved quickly to investigate, respond, and confirm the security of our systems. Specifically, Skokie: (1) installed Huntress endpoint protection; (2) installed SentinelOne (S1) Advanced Endpoint Detection; (3) reset all passwords, including those of domain and privileged accounts; (4) and updated all Firewalls.



00001020380000

P

Skokie will continue to take steps to mitigate the risk of future harm. In response to the Event, we are providing you with access to Credit Bureau Monitoring services at no charge for twelve (12) months. These services provide you with alerts when changes occur to your TransUnion credit file and starts from the date of enrollment. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

To enroll in Credit Monitoring services at no charge, please log on to: **<https://bfs.cyberscout.com/activate>** and follow the instructions provided. When prompted please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 1-800-405-6108 (toll free) Monday through Friday, during the hours of 8 a.m. and 8 p.m. Eastern Time (excluding U.S. national holidays).

Skokie sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,



John T. Lockerby
Village Manager
Village of Skokie

Steps You Can Take to Help Protect Your Information

Activate in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. Please note that the code is case-sensitive and will need to be entered as it appears.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Once enrolled you will have twelve (12) months of monitoring services. At the end of twelve (12) months, the services will be deactivated. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:



000010303000000

P

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-442-9828; and oag.dc.gov

For Maryland residents, the Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New York residents, the New York Department of State Division of Consumer Protection, Once Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 51-8-474-8553 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York's Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.