



**WEISSMANN ZUCKER
EUSTER + KATZ P.C.**
ATTORNEYS AT LAW

FOUNTAINS AT PIEDMONT CENTER
3495 PIEDMONT ROAD
BUILDING II, SUITE 950
ATLANTA, GEORGIA 30305
FACSIMILE: 404.364.2320

AUTHOR'S EMAIL: DKATZ@WZLEGAL.COM
DIRECT DIAL: 404.390.2941

April 22, 2022

Via Certified Mail; Return Receipt Requested

Consumer Protection Division
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: Cybersecurity Incident Involving City of St. Robert, Missouri (the "City").

Dear Consumer Protection Division:

Weissmann Zucker Euster + Katz, P.C. ("Weissmann Zucker") represents the City of St. Robert with respect to a recent cybersecurity incident that was first discovered on February 28, 2024 (hereinafter, the "Incident"). The City of St. Robert 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 residents being notified, and the steps the City 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 the Incident

On January 12, 2024, the City of St. Robert identified a localized attempt by unknown actors to obtain authentication credentials from employees of the City of St. Robert to their respective Microsoft Office 365 email accounts. City employees immediately reported this attempt and an investigation by a third-party cyber forensic investigation firm was initiated by the City. On February 28, 2024, this investigation identified one email account that was compromised as a result of cyber criminals obtaining such unauthorized access. The investigation determined that attackers may have acquired or accessed personally identifiable information as a result of obtaining access to this employee email account.

2. Number of Maryland resident affected.

A total of one (1) resident may have been potentially affected by this incident. A notification letter to this individual, was mailed on Tuesday April 23, 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 Incident.

The City 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, the City moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, JISD engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. In response to this incident the City has implemented Barracuda Email Gateway Defense, Content Shield and Impersonation Protection. The City has also implemented security awareness training for all City employees.

Although City is not aware of any actual or attempted misuse of the affected personal information, the City offered twelve (12) months of complimentary credit and dark web monitoring, a \$1,000,000 insurance reimbursement policy, and identity theft restoration services through Identity Defense to all individuals to help protect their identity. Further, the City 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

The City 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 dkatz@wzlegal.com or 404-918-5707.

Very truly yours,

A handwritten signature in black ink, appearing to read "David F. Katz", written in a cursive style.

David F. Katz

EXHIBIT A

Notification Letter to MD Consumer



PO Box 170500
Milwaukee, WI 53217

«name»
«primaddr»
«secaddr»
«city», «state» «zip»

April 23, 2024

NOTICE OF DATA BREACH

Dear «name»,

The City of St. Robert (“the City”) is writing to inform you of a data security incident that occurred on January 12, 2024, that resulted in unauthorized access to your personally identifiable information. While we have not received any reports of related identity theft since the date of the incident, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What happened?

On January 12, 2024, the City of St. Robert identified a localized attempt by unknown actors to obtain authentication credentials from employees of the City of St. Robert to their respective Microsoft Office 365 email accounts. City employees immediately reported this attempt and an investigation by a third-party cyber forensic investigation firm was initiated by the City. On February 28, 2024, this investigation identified one email account that was compromised as a result of cyber criminals obtaining such unauthorized access. The investigation determined that attackers may have acquired or accessed personally identifiable information as a result of obtaining access to this employee email account.

What Information Was Involved

Although the City has not received any reports of related identity theft since the date of the incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the following information may have been subject to unauthorized access or acquisition: name, date of birth, home address, driver’s license number, social security number, medical and health insurance information.

What We Are Doing.

Since the discovery of the incident, the City moved quickly to investigate, respond, and secure the information under our control. We are working to improve security measures, mitigate risk and have implemented additional safeguards to improve data security on our web server infrastructure. We are taking additional steps to protect City data from theft or similar criminal activity in the future.

What You Can Do.

To help relieve concerns and restore confidence following this incident, we have secured the services of Identity Defense to provide complimentary identity monitoring for 12 months. Please see the enclosed enrollment instructions to activate the services.

Affected individuals may consider freezing their credit to prevent loans, credit cards, and other services from being opened in their names without their permission. To initiate a credit freeze, contact each of the three national credit reporting agencies listed on the following page. Additional information is available at www.annualcreditreport.com.

We also recommend you review your credit reports and account statements over the next 12 to 24 months and notify your financial institution of any unauthorized transactions or incidents of suspected identity theft.

For More Information.

If you have any questions about this incident, please contact 1.877.411.4698, Monday – Friday between 9:00 a.m. and 6:00 p.m. Eastern Time, excluding major U.S. holidays. We deeply regret the concern or inconvenience this incident may cause you and appreciate your patience and support.

Sincerely,

Donald Coplin
Donald Coplin



«name»
Activation Code: «actcode»
Enrollment Deadline: July 21, 2024
Service Term: 12 months*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

To enroll in Identity Defense, visit <https://app.identitydefense.com/enrollment/activate/stro>

1. Enter your unique Activation Code <<IdentityDefenseID>>
2. Create Your Account
3. Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is July 21, 2024. If you do not enroll by July 21, 2024, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.888.217.0379.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Order Your Free Credit Report. 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 free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

Report Incidents. 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. If you detect any unauthorized transactions in a financial account, promptly notify your relevant financial institution or payment card company. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft: Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft/. If you believe your identity has been stolen, the FTC recommends that you take these steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently (for streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov/>); and (2) file a local police report, obtain a copy of the police report, and submit it to your creditors and any others that may require proof of the identity theft crime.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert stays on your credit file for one year and is a free service that helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Consider Placing a Security Freeze on Your Credit File. You may place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require you to provide certain personal information and proper identification prior to honoring your request to place a security freeze on your account. For example, you may be asked to provide: (1) Your full name with middle initial and generation (such as Jr., Sr., II, III); (2) your Social Security number; (3) your date of birth; (4) addresses where you have lived over the past five years; (5) a legible copy of a government-issued identification card (such as a state driver’s license or military ID card); and, (6) proof of your current residential address (e.g., current utility bill or account statement). Below is contact information for the three major credit bureaus:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-680-7289

Additional Information: This notification was not delayed due to a law enforcement investigation. **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).

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Contact the District of Columbia Office of Attorney General for steps to avoid identity theft: (202) 727-3400, 400 6th Street, NW, Washington DC 20001, <http://oag.dc.gov>.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Maryland 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/>.

Massachusetts Residents: You have the right to obtain a police report and request a security freeze (free of charge) as described above.

New York Residents: You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755 or 1-800-7889898; <https://ag.ny.gov/>. You also may contact the Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology>.

North Carolina Residents: You can obtain information from the North Carolina Attorney General’s Office about preventing identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; www.ncdoj.gov.

Oregon Residents: We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 or 1-503-378-4400; www.doj.state.or.us.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. 1 Rhode Island resident was notified of this incident.

South Carolina Residents: You can obtain information from the South Carolina Department of Consumer Affairs: 293 Greystone Blvd., Ste. 400, Columbia, SC 29210; 800-922-1594; www.consumer.sc.gov.

Texas Residents: You can obtain information from the Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; www.texasattorneygeneral.gov/consumer-protection/.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General’s Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

New Mexico: You have rights pursuant to the Fair Credit Reporting Act. These rights include knowing what is in your file and your credit score; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; to be told if information in your credit file has been used against you; as well as other rights. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. For more information about the FCRA, and your rights pursuant to the FCA, please visit https://files.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.