EXHIBIT 1

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the City of St. Cloud, Florida (the "City") does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 25, 2024, the City became aware of suspicious activity in its computer environment. The City promptly took steps to secure its systems and launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that between March 17, 2024 and March 25, 2024, an unauthorized actor gained access to certain systems and obtained certain information. In response, the City undertook a comprehensive review to determine what information was involved and to whom such information relates. Thereafter, the City also worked to validate the results, as well as to confirm the identities of, and appropriate contact information for, those potentially impacted. The City completed this process on April 28, 2025, and then moved as quickly as possible to provide notice.

The types of personal information related to Nebraska residents that were potentially impacted include: name, and driver's license number.

Notice to Nebraska Resident

On or about May 29, 2025, the City provided written notice of this event to potentially impacted individuals for whom it had complete address information, including approximately one (1) Nebraska resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the activity, the City moved quickly to investigate and respond to the event, assess the security of City systems, and identify potentially affected individuals. Further, the City notified federal law enforcement and is also working to implement additional safeguards and training to its employees. The City is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, the City is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. The City is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

The City is providing written notice of this incident to relevant state and federal regulators, as required, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

<<First Name>> <<Middle>> <<Last Name>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

May 29, 2025

NOTICE OF <<Variable Text 1: SECURITY INCIDENT/DATA BREACH>>

Dear <<First Name>> <<Middle>> <<Last Name>> <<Suffix>>:

The City of St. Cloud, Florida (the "City") writes to notify you of an event that may involve some of your information. Although we have not received any indication of identity theft or fraud involving your information, this letter provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or about March 25, 2024, the City became aware of suspicious activity in its computer environment. We promptly took steps to secure our systems and launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. Our investigation determined that between March 17, 2024 and March 25, 2024, an unauthorized actor gained access to certain systems and obtained certain information. In response, the City undertook a comprehensive review to determine what information was involved and to whom such information relates. Thereafter, the City also worked to validate the results of its review and locate address information for potentially affected individuals. We recently completed this process and then moved as quickly as possible to provide notice.

What Information Was Involved? Our investigation determined that the following types of information related to you were potentially impacted: your name and <<Variable Text 3: Data>><<Variable Text 3: Data Continue>>.

What We Are Doing. We take this event and information security very seriously. Upon learning of this event, we moved quickly to investigate and respond to the event, assess the security of the City's computer environment, and notify potentially affected individuals. As part of our ongoing commitment to information security, we are also reviewing our existing policies and procedures and implementing additional administrative and technical safeguards to further secure the information in our care. We also reported this event to appropriate government regulators, as required. As an added precaution, we are also offering you immediate access to credit monitoring and identity theft protection services for <<12/24>> months, through IDX, at no cost to you. We encourage you to enroll in these services as we are unable to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to detect errors. Any suspicious activity should be promptly reported to your credit card company, bank, or other applicable institution. In addition, you can enroll in the free credit monitoring and identity theft protection services that we are providing through IDX. Please note, you must enroll by August 29, 2025 to take advantage of these services. You can review the enclosed *Steps You Can Take to Help Protect Your Information* for enrollment instructions and to learn helpful tips on steps you can take to protect against possible information misuse.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions or need assistance, please call 1-800-939-4170 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. You may also write to the City at City of St. Cloud, City Clerk's Office, 1300 9th Street, St. Cloud, FL 34769.

Sincerely,
The City of St. Cloud, Florida

Steps You Can Take To Help Protect Your Information

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit 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:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/get-credit-report https://www.transunion.com/credit-freeze https://www.transunion.com/fraud-alerts
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, PO Box 2000 Chester, PA 19016

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; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. If you wish to verify the legitimacy of this letter, you may also contact the City of St. Cloud, Florida by calling 407-957-7359 or writing to us at The City of St. Cloud, City Clerk's Office, 1300 9th Street, St. Cloud, FL 34769. For all other inquiries, please call 1-800-939-4170.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 New York residents, the New York 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.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 4 Rhode Island residents that may be impacted by this event.