LAW OFFICES
CRENSHAW, WARE & MARTIN, P.L.C.
150 WEST MAIN STREET, SUITE 1923
Norfolk, Virginia 23510
www.cwm-law.com

TELEPHONE (757) 623-3000
FACSIMILE (757) 623-5735

DARIUS K. DAVENPORT
EMAIL: ddavenport@cwm-law.com
Also licensed in Wisconsin

April 15, 2026

Office of the New Hampshire Attorney General
Department of Justice
1 Granite Place South
Concord, NH 03301

Dear Attorney General Formella:

In accordance with New Hampshire Revised Statutes § 359-C:19-21, please accept this letter as our notice to the Attorney General's Office.

On or about February 25, 2026, the City of Suffolk, (the "City") became aware that it was the victim of a ransomware attack. Immediately, the City's management engaged third-party cybersecurity experts to investigate the incident, secure personal information, and protect the City's network from compromise. Law enforcement was notified, and an investigation was initiated to determine the nature and scope of the incident.

To date, our investigation revealed that malicious actors gained access to the City's network on or about February 24, 2026, and attempted to deploy ransomware. The threat actors were able to gain access to a limited set of data from the City's network before being detected. We cannot validate, with specificity, the data that the malicious actors gained access to; however, the City has compiled a list of 53 potentially affected individuals. To date, there is no evidence that personal information from any potentially affected individual has been misused.

Out of an abundance of caution and in accordance with New Hampshire law, the City is notifying those that we reasonably believe were potentially affected. The notices to those potentially affected will contain information about the incident, how to protect themselves, and how to obtain free credit reports. The draft notice letter is enclosed herein.

Notice to the Attorney General was delayed due to the City's ongoing efforts to identify affected individuals from systems that were encrypted during the ransomware attack.

For further information about this data incident, you may contact Darius Davenport, at ddavenport@cwm-law.com.

Sincerely,

Darius Davenport
Data Breach Counsel

April XX, 2026

The City of Suffolk (the "City") writes to notify you of a data security incident that may have impacted you. This notice is to inform you about the incident, our response, and steps you may take to protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? On or about February 25, 2026, the City became aware that it was the victim of a data incident. Immediately, the City's management, IT and third-party cybersecurity experts were engaged to investigate the incident, secure personal information and protect the City's network from compromise.

To date, our investigation revealed that malicious actors gained access to the City's data on or about February 24, 2026, and attempted to deploy ransomware to encrypt portions of the network. The malicious actor's network access was terminated soon after it was detected. Since an unknown actor gained access to our network data, we are providing this notice out of an abundance of caution. To date, we have not received any indication that your information was misused by an unauthorized individual.

What Information Was Involved? It is possible that your full name or first initial and last name combined with your Social Security number, passport number or financial account information may have been seen or accessed. This information is called your personally identifiable information. It tells others about you and is a part of your identity.

What We Are Doing. We take the confidentiality, privacy, and security of information in our care seriously. Upon discovering the incident, information technology experts were immediately engaged and commenced an investigation to determine the nature and scope of the incident. Additionally, we have reported the attack to the Federal Bureau of Investigation (FBI) Cyber Division and the Virginia Fusion Center, and we are committed to fully supporting any law enforcement investigations. While the investigation remains ongoing, we are taking steps now to implement additional safeguards and review policies and procedures relating to data privacy and security.

The City has implemented additional security measures designed to further protect the privacy of our citizens and staff. Among other steps taken, we engaged a leading security service provider to monitor our network, review our system's architecture, and implemented stronger policies to prevent future attacks.

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 activity. We also encourage you to review the "Steps You Can Take to Help Protect Your Information" pages enclosed herein.

For More Information. We understand that you may have some questions about this incident that are not addressed in this letter. Should you have additional questions, please contact the City [INSERT NUMBER].

We apologize for any inconvenience that may have arisen as a result of this incident and appreciate your understanding as we have worked to resolve this issue.

Sincerely,

Kevin Hughes
City Manager

Steps You Can Take to Help Protect Your Information

Check Your Accounts

We urge you to stay alert for incidents of identity theft and fraud, review your account statements, and check your credit reports for suspicious activity. Under U.S. law, you are eligible for one free credit report each year from each of the three major credit reporting bureaus. To order your free credit report, visit annualcreditreport.com or call toll-free 877-322-8228. You may also reach out to the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a security freeze on your credit report. The security freeze will stop a consumer reporting agency from giving out personal or financial information in your credit report without your consent. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Note: using a security freeze to take control over who gets access to your credit report may delay or prevent any new loan, credit, mortgage, or any other credit extension request or application you make from being approved timely. Under federal law, you cannot be charged to place or lift a security freeze on your credit report. If you wish to place a security freeze, please reach out to these major consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
888-397-3742	888-909-8872	800-685-1111
experian.com/freeze/center	transunion.com/credit-freeze	equifax.com/personal/credit-report-services

To request a security freeze, you will need to provide these items:

1. Your full name with middle initial and suffix (Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. The addresses where you have lived over the last five years, if you have moved
5. Proof of current address, such as a current utility bill or telephone bill
6. A clear photocopy of a government-issued identification card (state driver's license or ID card, military ID, etc.)
7. If you are a victim of identity theft, show a copy of either the police or investigative report or complaint to a law enforcement agency about identity theft

Instead of a security freeze, you have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Businesses are required to take steps to verify a consumer's identity before extending new credit once they see a fraud alert on a credit file. If you are a victim of identity theft, you are eligible for

an extended fraud alert. This is a fraud alert lasting seven years. If you wish to place a fraud alert, please reach out to any one of these agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
888-397-3742	800-680-7289	888-766-0008
experian.com/fraud	transunion.com/fraud-victim-resource/place-fraud-alert	equifax.com/personal/credit-report-services

More Information

You can learn more about identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by reaching out to:

- The consumer reporting agencies.
- The Federal Trade Commission at: 600 Pennsylvania Ave. NW, Washington, DC 20580, identitytheft.gov, 877-ID-THEFT (877-438-4338); TTY: 866-653-4261.
    - The FTC also urges those who learn their information has been misused to file a complaint with them. Reach out to the FTC for steps to file such a complaint.
- Your state Attorney General.

You have the right to file a police report if identity theft or fraud ever happen to you. Note: to file a report with law enforcement for identity theft, you will need to give some proof you have been a victim. Also, you must report cases of known or presumed identity theft to law enforcement and your state Attorney General.

All U.S. Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580, consumer.gov/idtheft, 877-IDTHEFT (877-438-4338), TTY: 866-653-4261.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, 888-743-0023 or 410-528-8662.

Washington D.C. Residents: Reach the Office of Attorney General for the District of Columbia at: 400 6th St. NW, Washington, DC 20001; 202-442-9828; https://oag.dc.gov.

California Residents: Visit the California Office of Privacy Protection (oag.ca.gov/privacy) for more information to protect yourself against identity theft.

Florida Residents: Office of the Attorney General of Florida, 1-866-966-7226 (Fraud Hotline), http://myfloridalegal.com/identitytheft.

Also, under the Fair Credit Reporting Act:

- The consumer reporting agencies must correct or delete wrong, lacking, or unverifiable information.
- The consumer reporting agencies may not report outdated bad information.
- Access to your file is limited.
- You must give your consent for credit reports to be given to employers.
- You may limit "prescreened" credit and insurance offers you get based on information in your credit report.
- You may seek damages from a violator.

You may have more rights under the Act not reviewed here. Identity theft victims and active duty military personnel have more specific rights under the Act. You can review your rights under the Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

New York Residents: Contact the Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 800-771-7755; https://ag.ny.gov.

North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 919-716-6400, 877-566-7226 (toll free within NC).

Oregon Residents: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, www.doj.state.or.us, 877-877-9392.