City of Rocky Mount – System Disruption Update
September 1, 2020

On August 14, 2020, the City of Rocky Mount discovered that certain City systems were infected with a malware impacting our ability to access those systems. The City immediately launched an investigation and notified law enforcement. Although this investigation is ongoing, the City has learned it was the victim of a sophisticated ransomware attack. Fortunately, the City maintained backup copies of impacted systems and data which is allowing the City to securely restore systems and City services. Throughout this incident, the City's emergency services continued to function, and the City has made significant progress in safely restoring other City services.

The City of Rocky Mount continues to investigate the full nature and scope of the recent cyber-attack and provides additional information about the incident and steps individuals can take to protect their personal information from possible misuse, should they feel it appropriate to do so.

In addition to causing a computer system disruption, the group responsible for this cyber-attack claim to have stolen City information and are threatening to publicly release the information unless the City pays a ransom. After consulting with our incident response partners, and at the recommendation of the FBI, the City refused to pay the ransom demand.

Please know that the City is dedicating all its resources to determining how this event occurred and what information is potentially impacted. However, the general categories of information maintained by the City varies by individual (e.g., employee, customer, resident, or vendor) but may include the following: name, Social Security number, driver's license / identification card number, financial account information, credit/debit card number, digital signature, electronic identification number, and/or email address/username and password.

Information security is among the City's highest priorities, and the City is actively working to implement additional security measures to prevent a similar incident from happening in the future. Although the City is unable to confirm at this time the type of information potentially at risk, in an abundance of caution, the City is providing the following information regarding steps individuals can take to protect their information from potential fraud or misuse:

Enroll in Credit Monitoring

The City of Rocky Mount has secured the services of Kroll to provide one year of credit monitoring for potentially impacted individuals at no cost. To get information on how you can enroll, call 877-461-2592.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud and to monitor your account statements and credit reports. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact 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, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Chester, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111

www.experian.com/freeze/center.html www.transunion.com/credit-freeze www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to 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 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Reset Online Account Passwords

As a general practice, the City encourages individuals to frequently reset online account passwords, to use complex password combinations, and to not share passwords or use identical passwords for multiple online accounts. Although the City's investigation has not confirmed that online account passwords were impacted by this event, the City encourages individuals to reset any online account passwords for accounts associated with the City or online accounts accessed while on the City's network or computer devices.

Additional Information

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 North Carolina Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, and www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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), 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. 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 to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

For More Information

The City greatly appreciates your patience as we continue to recover from this unprecedent event and regrets any concern you may have. If you have questions about this incident, we established a dedicated assistance line at 877-461-2592 which can be reached Monday through Friday from 9 a.m. to 5 p.m. Eastern Time.