



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

## Notice of Data Breach

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

We value our relationship with you and take the security of your data seriously. We are writing to inform you about the occurrence of a data security incident that may have involved some of your personal data, which is stored on servers belonging to the Cooke County Sheriff's Department. We want to further inform you that the Cooke County Incident Response Team has taken immediate and appropriate actions to reinforce existing security measures and to mitigate the potential impact of the incident. We want to reassure you that all critical functions of the Sheriff's Department are operational. Meanwhile, please review the information provided in this letter for some steps that you may take relating to this incident.

## What Happened?

On Saturday, July 4, 2020, the Cooke County Information Technology Department detected that an unauthorized third party conducted a ransomware attack on five of the Sheriff's Department's servers. The incident has been contained and is being thoroughly investigated. Immediately upon detecting the attack, the Cooke County Incident Response Team notified the Texas Department of Information Resources (DIR) about the encrypted servers and engaged the services of a forensics investigation firm, offered by DIR, to investigate the cause of the encryption and to contain the infection from spreading.

The forensics firm arrived onsite on Sunday, July 5, 2020, and notified law enforcement about the incident. Law enforcement immediately became involved to assist with the investigation. On or about Monday, July 6, 2020, the Cooke County Incident Response Team engaged an outside law firm to provide legal advice and direction in support of the incident response and engaged a Managed Security Services firm to restore the servers and enhance the security of the network.

After a detailed review of the server images and images of affected computers, the Cooke County Incident Response Team was finally able to determine, on Friday July 17, 2020, that some of the databases and folders on the servers of the Sheriff's Department contain personal information and that those data folders and case files were accessed, copied, and sent to an external server controlled by the unauthorized third party. Law enforcement instructed the Cooke County Incident Response Team to delay formal public notification until Monday, July 20, 2020 to avoid retaliation by the unauthorized users over the weekend. However, this notification to you was not delayed as a result of that request by law enforcement.

## What Information Was Involved?

While we could not determine whether your specific personal information was used by an unauthorized third party, we are notifying you of this incident out of an abundance of caution because data folders and case files containing your personal information on the servers, were accessed and copied by an unauthorized third party. More specifically, the data folders and case files may have contained your name, date of birth, social security number, and/or driver's license number.

## What We Are Doing

The Cooke County Incident Response Team hired an expert outside IT Forensics firm to investigate the ransomware attack, determine the scope of it, and respond to it. In addition, the Cooke County Incident Response Team implemented several of the Managed Security Services firm's recommendations for hardening its systems and has scheduled other steps designed to enhance the security of the Cooke County Sheriff's network.

Additionally, to help relieve your concerns and restore your confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

*You have until **November 10, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

## What You Can Do

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

## For More Information

We sincerely apologize for any inconvenience or concern this incident may cause. If you have questions, please call 1-844-925-2473, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready or send us an email at [privacy@co.cooke.tx.us](mailto:privacy@co.cooke.tx.us).

Sincerely,



Jason Brinkley  
Cooke County Judge

## **Additional Resources**

**Review Accounts and Credit Reports:** It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. 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 annual free credit report please visit **[www.annualcreditreport.com](http://www.annualcreditreport.com)** or call toll free at **1-877-322-8228**. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

**For residents of Maryland:** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us).

**For residents of North Carolina:** You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, [www.ncdoj.gov](http://www.ncdoj.gov).

**For residents of Rhode Island:** You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, <http://www.riag.ri.gov>.

### **Security Freezes and Fraud Alerts:**

You have a 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. There is no fee for a security freeze. 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.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

**Additional Information for Massachusetts Residents:** Massachusetts law gives you the right to place a security freeze on your consumer reports. By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and an incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should

be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

**Additional Information for New Mexico Residents:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under the FCRA:

- You have the right to be told if information in your file has been used against you;
- You have the right to receive a copy of your credit report and the right to ask for a credit score;
- You have the right to dispute incomplete or inaccurate information;
- You have the right to dispute inaccurate, incomplete, or unverifiable information;
- You have the right to have outdated negative information removed from your credit file;
- You have the right to limit access to your credit file;
- You have the right to limit “prescreened” offers of credit and insurance you get based on information in your credit report;
- You have the right to seek damages from violators; and
- You have the right to place a “security freeze” on your credit report.

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and may need to provide all of the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity; and
- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of pre-screening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For more information, including information about additional rights, you can visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>, <https://www.consumerfinance.gov/learnmore/>, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com) <b>General Contact:</b> P.O. Box 740241 Atlanta, GA 30374 800-685-1111 <b>Fraud Alerts:</b> P.O. Box 740256 Atlanta, GA 30374 <b>Credit Freezes:</b> P.O. Box 105788 Atlanta, GA 30348	Experian (www.experian.com) <b>General Contact:</b> P.O. Box 2002 Allen, TX 75013 888-397-3742 <b>Fraud Alerts and Security Freezes:</b> P.O. Box 9554 Allen, TX 75013	TransUnion (www.transunion.com) <b>General Contact, Fraud Alerts and Security Freezes:</b> P.O. Box 2000 Chester, PA 19022 888-909-8872
--	---	---



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.