



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Security Incident

Dear <<Name 1>>:

The Caddo Parish District Attorney’s Office (the “Caddo DA”) is writing to inform you of a recent incident that may impact the privacy of some of your personal information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the incident, our response, and steps you may take to protect against any misuse of your information, should you feel it necessary to do so.

What Happened?

On or about October 25, 2021, the Caddo DA became aware of suspicious activity on its network and discovered that it could not access certain files and folders on its servers. The Caddo DA immediately launched an investigation to determine the nature and scope of the incident. The investigation determined that certain computer systems on the Caddo DA network had been infected by malware. The investigation was unable to rule out unauthorized access to, or taking of, information stored on the Caddo DA network. Out of an abundance of caution, the Caddo DA is providing notice of this incident to current or former employees, as well as their beneficiaries or dependents, whose personal information was stored within the Caddo DA network at the time of the incident.

What We Are Doing.

We take this incident and the security of personal information in our care very seriously. Upon discovery of this incident, the Caddo DA immediately took steps to ensure the security of our systems and investigate the incident. As part of our ongoing commitment to the privacy of information in our care, we are implementing additional technical security measures to strengthen the security of our systems. We are also reviewing and enhancing our existing data privacy policies and procedures.

As an added precaution, we are offering you access to twelve (12) months of credit monitoring and identity theft protection services through Equifax at no cost to you. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Protect Personal Information*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud, to monitor your accounts for any unusual activity, and to report any instances of theft or fraud to law enforcement. You can also enroll to receive the complimentary credit monitoring services that we are offering to you.

For More Information.

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 855-604-1778. This toll-free line is available Monday – Friday from 9:00 AM and 9:00 PM Eastern time.

Sincerely,

The Caddo Parish District Attorney's Office

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

1. Enrolling in Complimentary 12-Month Credit Monitoring.



Enter your Activation Code: **<ACTIVATION CODE>**
Enrollment Deadline: **<DEADLINE MMMM DD, YYYY>**

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of **<ACTIVATION CODE>** then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. ²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com ⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 one-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 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 your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

EXHIBIT B

NOTICE OF DATA SECURITY INCIDENT

The Caddo Parish District Attorney's Office (the "Caddo DA") learned of an incident that may affect the privacy of certain information. The Caddo DA is providing notice of this incident so potentially affected individuals may take steps to better protect their personal information, should they feel it appropriate to do so.

What Happened? On or about October 25, 2021, the Caddo DA became aware of suspicious activity on its network and discovered that it could not access certain files and folders on its servers. The Caddo DA immediately launched an investigation to determine the nature and scope of the incident. The investigation determined that certain computers on the Caddo DA network had been infected by malware. The investigation was unable to rule out unauthorized access to, or taking of, information stored on the Caddo DA network. However, there is no evidence to indicate that any accessed data has been misused. The Caddo DA has undertaken a lengthy and labor-intensive process to identify the information within the affected systems and address information associated with the affected individuals.

What Information Was Involved? The information that could have been subject to unauthorized access varies by individual and may include name, address, and one or more of the following: date of birth; Social Security number; U.S. alien registration number; passport number; driver's license or state-issued identification number; military identification number; tax identification number; tribal identification number; non-U.S. national identification number; copy of birth or marriage certificate; IRS pin number; student identification number; employer identification number; financial account information; payment card information; system access information; biometric data; worker's compensation information; medical information; or health insurance information.

What We Are Doing. We take this incident and the security of personal information in our care very seriously. Upon discovery of this incident, the Caddo DA immediately took steps to ensure the security of our systems and investigate the incident. As part of our ongoing commitment to the privacy of information in our care, we are implementing additional technical security measures to strengthen the security of our systems. We are also reviewing and enhancing our existing data privacy policies and procedures. The Caddo DA is working diligently to identify the individuals whose information may have been affected is a result of this incident and to provide them with further information regarding this incident.

What You Can Do. The Caddo DA encourages affected individuals to review and consider the information and resources outlined in the Steps You Can Take to Protect Your Personal Information addressed below.

For More Information. We understand that you may have questions about this incident. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 855-604-1778. This toll-free line is available Monday – Friday from 9:00 AM and 9:00 PM Eastern Time.

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

The Caddo DA encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud and to review account statements, credit reports, and explanation of benefits forms for suspicious activity.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 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 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 your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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/credit-reporting/help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. The Caddo Parish District Attorney's Office is located at 501 Texas St., 5th Floor. Shreveport, Louisiana 71101.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your 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, you have the right to obtain any police report filed in regard to this incident. There are seven [7] Rhode Island residents impacted by this incident.

EXHIBIT C

The Caddo Parish District Attorney's Office Provides Notice of Privacy Incident

NEWS PROVIDED BY

The Caddo Parish District Attorney's Office →

Mar 15, 2022, 16:47 ET

SHREVEPORT, La., March 15, 2022 /PRNewswire/ -- The Caddo Parish District Attorney's Office (the "Caddo DA") is providing notice of an incident that may affect the security of some information relating to certain individuals associated with the Caddo DA. The confidentiality, privacy, and security of information in the Caddo DA's care is among its highest priorities and the Caddo DA takes this incident very seriously. Please note, the Caddo DA has no indication that anyone's information has been subject to actual or attempted misuse in relation to this incident.

On or about October 25, 2021, the Caddo DA became aware of suspicious activity on its network and discovered that it could not access certain files and folders on its servers. The Caddo DA immediately launched an investigation to determine the nature and scope of the incident. The investigation determined that certain computers on the Caddo DA network had been infected by malware. The investigation was unable to rule out unauthorized access to, or taking of, information stored on the Caddo DA network. The Caddo DA has undertaken a lengthy and labor-intensive process to identify the information within the affected systems and address information associated with the potentially affected individuals.

The Caddo DA determined, through its investigation, that the information potentially at risk varies by individual and may include certain individuals' name, address and one or more of the following: date of birth; Social Security number; U.S. alien registration number; passport number; driver's license or state-issued identification number; military identification number; tax identification number; tribal identification number; non-U.S. national identification



number; copy of birth or marriage certificate; IRS pin number; student identification number; employer identification number; financial account information; payment card information; system access information; biometric data; worker's compensation information; medical information; or health insurance information.

The Caddo DA has seen no indication that any information has been subject to actual or attempted misuse in relation to this incident.

The Caddo DA takes this incident and the security of personal information in its care very seriously. Upon discovery of this incident, the Caddo DA immediately took steps to ensure the security of its systems and investigate the incident. As part of its ongoing commitment to the privacy of information in its care, it is implementing additional technical security measures to strengthen the security of its systems. The Caddo DA is also reviewing and enhancing its existing data privacy policies and procedures. While unaware of misuse or any personal information, on March 15, 2022, the Caddo DA mailed notice letters to affected individuals for whom it had sufficient contact information. In addition to notifying impacted individuals, the Caddo DA is also reporting to regulatory officials, as required. As a precaution, the Caddo DA is also offering impacted individuals with credit monitoring services through Equifax at no cost.

The Caddo DA encourages impacted individuals to remain vigilant against incidents of identity theft and fraud, to review their account statements, and to monitor their credit reports for suspicious activity. The Caddo DA is providing potentially impacted individuals with contact information for the three major credit reporting agencies, as well as providing advice on how to obtain free credit reports and how to place fraud alerts and security freezes on their credit files.

The relevant contact information is below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes, and the steps they may take to protect their information by contacting the credit bureaus, the Federal Trade Commission or their state Attorney General. 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.

Instances of known or suspected identity theft should also be reported to law enforcement or the individual's state Attorney General.

The Caddo DA has established a dedicated call center for individuals to contact with questions or concerns or to determine if they are impacted. This dedicated call center can be reached at 855-604-1778 Monday through Friday, 9:00 AM – 9:00 PM Eastern Time.

SOURCE The Caddo Parish District Attorney's Office