

eClinicalWorks

September 6, 2023

BY EMAIL

Office of the Attorney General
Attorney General Anthony G. Brown
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Email Incident

Dear General Brown,

We are writing to share information regarding a recent incident at eClinicalWorks (“eCW”) that may have impacted the personal information of **four** Maryland residents.

An unauthorized third party gained access to two eCW email inboxes. The inboxes contained some emails from corporate clients requesting to make one-time credit card payments. The information that may have been accessed during the incident included name, address, credit card number, expiration date, and security code. Further, eCW has reason to believe the unauthorized third party’s primary purpose was to access business information, not credit card authorization emails; as a result, there has been no indication that anyone has accessed or misused the information.

The unauthorized third party had browser-based access to the email inboxes from approximately November 1, 2022 to December 10, 2022. Upon discovering the incident in December 2023, eCW conducted an investigation into the incident and engaged a third-party firm, who confirmed that the incident was limited to the two inboxes in the email system. At that point, eCW began to analyze the contents of the two inboxes, which involved a time-consuming, largely manual review of thousands of emails.

eCW maintains a written information security program and has implemented further safeguards, including additional security applications, dark web monitoring, and regular purging of emails containing financial information.

eCW sent a communication to its corporate clients on December 19, 2023 encouraging them to be vigilant and to report any phishing attempts to eCW immediately. In addition, upon completion of the investigation, eCW is preparing notices to those individuals whose credit card information may have been accessed by the unauthorized party. A sample of the individual notification to be sent on September 7, 2023, is attached to this letter.

If you have any questions, please contact me at 508-475-0450 or privacy@eclinicalworks.com.

Sincerely,

Nainil Chheda
Privacy Officer
eClinicalWorks
2 Technology Drive, Westborough, MA 01581
www.eClinicalWorks.com

eClinicalWorks

Practice Name
Attn: Name
Address
City, State Zip

Re: Email Incident

Dear [Insert Name]:

We are writing to share with you some important information regarding an email incident that may have impacted your personal information. We have no indication that your specific information was accessed or misused, but we are providing this notice in the interest of transparency.

What Happened?

An unauthorized third party gained access to two email inboxes between November 2022 and December 2022. The inboxes contained an email from you requesting to make a one-time credit card payment.

We are not aware that the specific email including your information was accessed by the unauthorized individual; however, we are notifying you because eCW has determined that your information was available within the email account and we cannot rule out the possibility that it was accessed.

What Information Was Involved?

The information involved in the incident included name, address, credit card number, expiration date, and security code regarding the payment card you use for corporate transactions. Further, we do not have information indicating that the specific email containing your information was accessed or that any such information has been misused. Nevertheless, in the interest of transparency, we are providing this notice so that you are aware of the incident.

What We Are Doing.

eCW has conducted a thorough investigation into the incident and engaged a third-party firm, who confirmed that the incident was limited to two inboxes in the email system. We have instituted additional safeguards and will continue to monitor the eCW email system.

What You Can Do

If you are contacted by anyone you do not know at eCW requesting personal information, please do not share your information and let us know immediately.

Although we are not aware of any fraudulent activity associated with your personal information, it is always advisable to regularly review your financial accounts and report any suspicious or unrecognized activity immediately. The enclosed "General Information About Identity Theft Protection" provides further information about what you can do. The inclusion of this information is not intended to suggest that you are at a substantial risk of harm. As recommended by federal regulatory agencies, you should be vigilant for the next 12 to 24 months and report any suspected incidents of fraud to the relevant financial institution.

eCW regrets this incident and any inconvenience to you. If you have any questions or would like additional information regarding this incident, please contact us at privacy@eclinicalworks.com.

Sincerely,

Nainil Chheda
Privacy Officer
eClinicalWorks
2 Technology Drive, Westborough, MA 01581
www.eClinicalWorks.com

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

It is always advisable to regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below:

- **Equifax**, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com
- **Experian**, P.O. Box 9532, Allen, TX 75013. 1.888.397.3742. www.experian.com
- **TransUnion**, 2 Baldwin Pl., P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. www.transunion.com

Fraud Alert: You may contact the fraud department of the three major credit bureaus to request that a “fraud alert” be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.800.685.1111
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.680.7289

Security Freeze for Credit Reporting Agencies: You may request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. It is free to place, lift or remove a security freeze. You must separately place a security freeze on your credit report at each credit bureau. To do so, you must contact the credit bureaus by phone, mail, or secure electronic means:

- **Equifax:** P.O. Box 105788, Atlanta, GA 30348, 1.800.349.9960, www.Equifax.com
- **Experian:** P.O. Box 9554, Allen, TX 75013, 1.888.397.3742, www.Experian.com
- **TransUnion:** P.O. Box 2000, Chester, PA 19106, 1.888.909.8872, www.TransUnion.com

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- 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

If you request a freeze online or by phone, the agency must place the freeze within one business day. The credit bureaus have three business days after receiving a request by mail to place a security freeze on your credit report, and they must also send confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must contact the credit reporting agencies and include (1) proper identification; (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities

of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

You also have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information.

Steps You Can Take if You Are a Victim of Identity Theft

- **File a police report.** Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- **Contact the U.S. Federal Trade Commission (FTC).** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <https://www.identitytheft.gov/#/>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.
- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is helpful to log conversations with creditors, law enforcement officials, and other relevant parties.

Additional Steps to Avoid Identity Theft: The FTC has further information about steps to take to avoid identity theft at: <https://consumer.ftc.gov/features/identity-theft>; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

State Specific Information

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.oag.state.md.us/idtheft/index.htm>, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

New York residents can learn more about security breach response and identity theft prevention and protection from the New York State Department of State Division of Consumer Protection, by visiting their web site at <https://dos.ny.gov/protecting-yourself-identity-theft> or by contacting federal agencies using the contact information listed above.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <http://www.atg.state.vt.us>.