



November 21, 2024

Jennifer Stegmaier
312.821.6167 (direct)
Jennifer.stegmaier@wilsonelser.com

Via Email

Attorney General Anthony G. Brown

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Cybersecurity Incident Involving Central Carolina Insurance Agency

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Central Carolina Insurance Agency (“CCIA”), an independent insurance firm located at, Salisbury, NC 28147, with respect to a recent cybersecurity incident that was first discovered by CCIA on March 20, 2024 (hereinafter, the “Incident”). CCIA takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, and the steps that CCIA has taken in response to the Incident. We have also enclosed hereto a sample of the individual notice letter that will be mailed to affected individuals.

1. Nature of the Incident

On March 20, 2024, CCIA detected suspicious activity on its network. Upon discovery of this incident, CCIA immediately disconnected all access to the network and promptly engaged a specialized cybersecurity firm and IT personnel to assist with securing the environment, as well as to conduct a forensic investigation to determine the nature and scope of the incident. CCIA notified the FBI of the incident on March 28, 2024.

The forensic investigation concluded on or about April 23, 2024 and determined that an unauthorized third party gained access to CCIA’s network from December 31, 2023 to March 20, 2024 and accessed certain files. Based on these findings, CCIA began reviewing the affected systems and files to identify the specific individuals and the types of information that may have been compromised. On April 24, 2024, CCIA engaged a third-party data mining vendor to assist with reviewing this data. While this process was going, on May 17, 2024, CCIA posted a Substitute Notice to its website and published a Media Release in The Charlotte Observer. On November 13, 2024, CCIA received the final list of individuals to notify. Notice letters will be mailed to the affected individuals by U.S. first-class mail on November 21, 2024.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

Based on the investigation, the following information may have been subject to unauthorized access: first name/initial and last name; address; phone number; Social Security number; passport number; driver's license number; license plate/vehicle identification number; financial account number; credit card number; health insurance policy number; date of birth; and/or protected health information including patient ID number, medical records, birth certificate, green card, digitized or electronic signature, and/or hull ID number. In addition, there may have been unauthorized access to files containing usernames and passwords belonging to a few CCIA employees. Please note that the information varies among the affected individuals.

2. Impacted Individuals

CCIA identified 4 Maryland residents affected by this incident. Notification letters will be mailed to these individuals on November 21, 2024. A sample copy of the individual notification letter is included with this letter as **Exhibit A**.

3. Steps taken in response to the Incident

Data privacy and security is among CCIA's highest priorities, and it is committed to doing everything it can to protect the privacy and security of the personal information in its care. Since the discovery of the incident, CCIA moved quickly to investigate and respond to the Incident. Specifically, CCIA engaged a specialized cybersecurity firm and IT personnel to secure its environment and to conduct a forensic investigation to determine the nature and scope of the incident. Additionally, CCIA took the following steps, including but not limited to: disconnecting all access to their network, changing administrative credentials, restoring operations in a safe and secure mode, enhancing security measures, and took steps and will continue to take steps to mitigate the risk of future harm.

In response to the incident, CCIA is offering Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services provided by Cyberscout to all affected individuals at no charge. Individuals have ninety days from the date of their notification letters to enroll in these complimentary services. These services are provided for twelve months from the date of enrollment. The complimentary services also include proactive fraud assistance to help with any questions.

3. Contact information

CCIA remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Jennifer.Stegmaier@wilsonelser.com or 312-821-6167.



Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

A handwritten signature in black ink, appearing to read 'Jennifer Stegmaier'. The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Jennifer S. Stegmaier

Exhibit A

Sample Individual Notice Letter

Central Carolina Insurance Agency
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Via First-Class Mail

P



November 21, 2024

Re: Notice of Data Breach

Dear [REDACTED],

Central Carolina Insurance Agency (“CCIA”) is writing to inform you of a recent data security incident that may have resulted in an unauthorized access to your sensitive personal information. CCIA obtained certain of your personal information because CCIA is an insurance agent or producer for insurance policies that were applied for or issued which list you as a policyowner, insured and/or beneficiary.

We take the protection of your personal information very seriously and are sending you this notice to tell you what happened, what information was involved, what we have done in response, what you can do in response to this incident, and what resources are available to help protect against the potential misuse of sensitive personal information.

What Happened?

On March 20, 2024, CCIA detected suspicious activity on its network. Upon discovery of this incident, CCIA immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. CCIA notified the FBI of the incident on March 28, 2024. The forensic investigation concluded on or about April 23, 2024, and determined that an unauthorized third party accessed some of CCIA’s files without authority and that the unauthorized activity occurred between December 31, 2023, and March 20, 2024. On May 17, 2024, CCIA posted substitute notice on its website and published media notice in The Charlotte Observer.

Based on the forensic findings, CCIA began an extensive and comprehensive review of the affected files with the assistance of a specialized third-party data mining vendor to identify the specific individuals and the types of information that may have been compromised. On November 13, 2024, CCIA received final list of individuals to notify.

What Information Was Involved?

The following categories of your personal information may have been accessed by an unauthorized third party: full name, and financial account number. Please note the information impacted varies for each potentially impacted individual.

What We Are Doing

Data privacy and security is among CCIA’s highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the incident, CCIA moved quickly to investigate, respond, and confirm the security of our systems.

Specifically, CCIA engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident. We have also contacted and are cooperating with federal law enforcement authorities, and this notice has not been delayed due to law enforcement investigation. Additionally, we have taken a number of technical and administrative steps to further enhance the security of our system and data, including, but not limited to: disconnecting all access to the network; changing administrative credentials, restoring operations in a safe. CCIA has taken steps and will continue to take steps to mitigate the risk of future harm.

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do

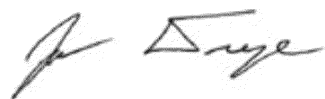
We encourage you to enroll in the complimentary credit monitoring services that CCIA is providing to you at no cost. We also recommend that you remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take recommended steps to protect your interests, including the possible placement of a free fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information* to learn more about how to protect against the possibility of information misuse.

For More Information

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-855-577-8197 and supply the representative with your unique code listed above.

CCIA sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,



John A. Drye, CPCU, CIC
Vice President
Central Carolina Insurance Agency

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed 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 for a fee by contacting one or more of the three national credit reporting agencies.



You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General’s office in your home state and you have the right to file a police report and obtain a copy of your policy report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting <https://oag.dc.gov>, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting <http://www.marylandattorneygeneral.gov/Pages/contactus.aspx>.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at <https://dos.nysits.acsitefactory.com/consumerprotection>; by visiting the New York Attorney General at <https://ag.ny.gov> or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or <https://www.identitytheft.gov/#/>.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.