Welts, White & Fontaine, P.C.—Notice of Data Security Incident

Welts, White & Fontaine, P.C. ("WWF") is a full-service law firm with approximately nine attorneys located in Nashua, New Hampshire. The privacy and security of the personal information we maintain is of the utmost importance to WWF.

On or around January 8, 2025, we learned that an unauthorized actor may have accessed our network and copied files from our file server. We immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to contain and secure our environment and to analyze the extent of any compromise of the files on our network. We also alerted law enforcement. Security is an ongoing process and we are continually taking steps to improve our safeguards to protect information in our network.

Based on our comprehensive investigation, on January 14, 2025 we discovered that the unauthorized actor likely copied some data from our network environment. While we do not process or sell personal data as part of our business, we occasionally receive documents containing personal information and protected health information during the normal course of providing legal services. We are mindful that our files have the potential to contain sensitive legal information, personal information, and protected health information associated with individuals. Therefore, we are providing this notice out of an abundance of caution.

To date, we are not aware of any incidents or reports of identity fraud or improper use of any information as a result of this incident. Nevertheless, we are providing the following steps individuals may take in order to protect themselves, including placing a fraud alert/security freeze on their credit files, obtaining free credit reports, remaining vigilant in reviewing financial account statements and credit reports for fraudulent or irregular activity, changing passwords, and taking steps to safeguard against medical identity theft. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security of our network and privacy of personal information.

Further, we are offering potentially impacted individuals access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. These services provide you with alerts for 12 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. These services are designed for individuals only, not businesses. Please contact us at (603) 546-1621 to request a complimentary code for these services.

At WWF, protecting the privacy of personal information is a top priority. WWF is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. WWF continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information. Should you have any questions regarding this notification, please contact us at (603) 546-1621. Thank you for your cooperation.

– OTHER IMPORTANT INFORMATION –

Enrolling in Complementary 12-Month Credit Monitoring.

For individuals that received a credit monitoring code, 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 your unique code to receive services. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this notice. 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.

Placing a Fraud Alert on Your Credit File.

You may choose to place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

Consider Placing a Security Freeze on Your Credit File.

You may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888)-298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online

at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Protecting Your Medical Information.

As a general matter, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.

- Change passwords to any online portals for any medical providers.

- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

###