

Wettermark Keith, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Exhibit A



October 1, 2025

Notice of Data Security Incident

Dear [REDACTED],

We are writing to inform you of a data security incident that may have involved certain personal information related to your prior representation by our firm (Wettermark Keith LLC formerly Wettermark Holland and Keith LLC). You are receiving this letter either because you were a former client of our firm, you contacted our firm for consultation about a potential case, or you were part of a case associated with our firm. We take the privacy and security of your information seriously and sincerely apologize for any concern or inconvenience this may cause you. We want to explain what occurred, the steps we have taken, and what you can do to protect yourself.

What Happened?

On April 14, 2025, our firm experienced a cyber incident involving unauthorized access to portions of our internal computer system. We immediately implemented our incident response protocols, took our systems offline, and engaged computer forensic investigators to determine the scope of the incident. The forensic investigation determined some files from our network may have been accessed by an unauthorized actor during this incident. We worked with a vendor to review the files to identify any personal information. This review was completed on September 15, 2025, at which point we determined that your personal information may have been impacted. At this time, we are not aware of any misuse of your information. We are, however, writing you out of an abundance of caution to inform you of the incident and to provide you with resources to assist you in protecting your information.

What Information Was Involved?

The potentially impacted information may include your name and some combination of the following: Social Security number.

Please note that your case outcome and legal rights were not impacted. The incident only affected certain stored data and does not affect our prior representation of you.

What We Are Doing:

We take our responsibility to safeguard client information very seriously. As noted above, we immediately contained the incident and removed unauthorized access, conducted a full forensic investigation, removed your personal data from our internal servers, deployed enhanced monitoring software, changed all user and system passwords, and implemented other security controls.

In addition, and out of an abundance of caution to assist you, we are offering identity theft protection services through Transunion at zero cost to you through **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file.

000010102G0500

P

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:

Additional information about protecting your identity is included in this letter, 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. We also encourage you to take full advantage of this service offering. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident.

For More Information:

If you have any questions or concerns, please call **833-866-8693** Monday through Friday from 8 am - 8 pm Eastern Time excluding holidays and supply the fraud specialist with your unique code listed above. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Wettermark & Keith, LLC

Recommended Steps to Help Protect Your Information

1. Website and Enrollment.

You can enroll in the complimentary credit monitoring services being offered to you by logging on to <https://bfs.cyberscout.com/activate> and following the provided instructions. When prompted, please provide the following unique code: [REDACTED]. The enrollment requires an internet connection and email account and may not be available to minors. 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.



2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 agencies 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 a 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. You can 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.