Alten Sakai
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

Alten Sakai & Company LLP
8625 SW Cascade Avenue, Suite 310
Beaverton, Oregon 97008-7126
503.297.1072
altensakai.cpa

July 28, 2025

Notice of Data Security Incident

Dear [redacted]

We want to let you know about a recent data security incident that may have impacted your personal information. Alten Sakai & Co. LLP ("Alten Sakai") is an accounting firm and may have received your information for tax related purposes, such as filing tax returns. We take the privacy and security of your information seriously and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to you.

What Happened:

On May 19, 2025, we discovered suspicious activity on our systems. We immediately implemented our incident response protocols and engaged external cybersecurity specialists to help conduct an investigation and determine the scope and extent of the incident. The investigation determined that there was unauthorized access to some of our servers that store personal tax-related information. While we have no evidence that your personal information was misused, we wanted to inform you about this incident out of an abundance of caution.

What Information Was Involved:

The impacted information includes your name, address, social security number, date of birth and documents related to the preparation of your tax return, which could include financial account statements, bank account numbers and driver's license number, if provided.

What We Are Doing:

Since the incident we have taken steps to prevent a similar incident from occurring in the future, including deploying endpoint detection and threat monitoring software on all endpoints, changing all passwords and deploying enhanced security tools throughout our IT environment. We've also notified and are cooperating with law enforcement.

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 twenty-four (24) 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:

It is always a good idea to remain vigilant and be on the lookout for evidence of identity theft or fraud, and to review your bank account and other financial statement as well as your credit reports for suspicious activity for the next 12 to 24 months.

If you believe you are a victim of tax-related identity theft, the IRS recommends the following:

- Respond immediately to any IRS written notice. **The IRS will never contact you by phone.**
- If you received a letter from the IRS indicating that they received a suspicious tax return with your name on it, you should follow the instructions in that letter to verify your identity with the IRS. Once you verify your identity, you can advise the IRS that you did not file the suspicious tax return. Additionally, you may be asked to file a paper return for the current tax year.
- You can also apply for an IRS Identity Protection PIN (IP PIN). This is a 6-digit code issued by the IRS that is used to help prevent unauthorized tax filings using your Social Security number. Please contact Alten Sakai directly for assistance with setting this up.

We also encourage you to contact Cyberscout with any questions and take full advantage of the Cyberscout service offering. 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 **1-833-367-5015** and supply the fraud specialist with your unique code listed above. Additional information about protecting your identity is included in this letter, including recommendation 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.

For More Information:

Please call **1-833-367-5015** between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays with any questions. Your trust is important to us, and we regret any inconvenience or concern that this matter may cause you.

Sincerely,

Alten Sakai & Co. LLP

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

1. 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.

2. 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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	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.

3. 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.

4. 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.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

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/201904_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.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft.