Todd&Weld LLP
P.O. Box 989728
West Sacramento, CA 95798-9728

[redacted]

Enrollment Code: [redacted]

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
[redacted]

March 26, 2025

[redacted]

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Todd & Weld LLP. We want to notify you of an incident that may have involved your personal information. We are writing to provide you with information regarding the incident, advise you of the services we are making available to you, and reaffirm that Todd & Weld continues to take significant measures to protect personal information.

Why Does Todd & Weld Have my Information?
Todd & Weld received your information through the scope of its engagement with [redacted]

What Happened?
Todd & Weld recently detected unauthorized access to two employee email accounts as a result of a phishing email.

What We Are Doing.
Upon learning of this issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. The forensic investigation confirmed that two employee email accounts were accessed by an unauthorized individual between September 30, 2024 and October 23, 2024.

After an extensive forensic investigation and comprehensive manual review of the affected data, we discovered on January 22, 2025 that the compromised email accounts contained a limited amount of personal information and subsequently notified [redacted] of our investigation and findings on or about February 18, 2025. On March 6, 2025, we received updated address information from [redacted] and approval to provide you with notice of the incident.

What Information Was Involved?
The information potentially impacted includes your first and last name along with your [redacted]

What You Can Do.
While we have no evidence that any of the impacted information has been improperly used or disclosed, out of an abundance of caution, we want to make you aware of the incident. To help protect your information, we are offering complimentary identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: [redacted] months of credit and CyberScan monitoring, a $1,000,000

insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.
Our people and clients remain our top priority, and we will continue to work diligently to protect their confidential information. We take this situation very seriously and are taking all appropriate precautions to mitigate any potential harm. We continue to review our physical safeguards and address employee training.

If you have any further questions regarding this incident, please call our toll-free response line at [redacted] This response line is available Monday through Friday, 9:00 a.m. – 9:00 p.m. Eastern Time, excluding major US holidays.

Sincerely,

Todd & Weld LLP
[redacted]

OTHER IMPORTANT INFORMATION

1. Enrolling in Complimentary [redacted] Months Credit Monitoring.

Please enroll online or by phone.

Enrollment Code: [redacted]
Enrollment URL: [redacted]
Enrollment TFN: [redacted]
Deadline: June 26, 2025

IDX Identity enrollments will include [redacted] month enrollments into the following service components:

TRIPLE BUREAU CREDIT MONITORING (adults*) - Monitoring of credit bureaus for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY – IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned ID Care Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary [redacted] months credit monitoring services, we recommend that you 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	***Experian***	***TransUnion***
P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, 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
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960
(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 you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. 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.

5. 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 this 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.

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.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, Telephone: 888-743-0023.