**March 10, 2026**

**Dear Valued Client,**

We are writing to let you know about a data security incident at Melvin Mora & Associates, Income Tax + Business Services, Inc., that may have involved some of your personal information.

**What happened**

We learned of a nation-wide breach that affected our systems. The incident affected our 2025 client data environment in late February 2026. As part of this investigation, we identified thirteen (13) clients for whom fraudulent tax returns were filed using their information. Those returns have been reported and are blocked from being funded by the Internal Revenue Service and the California Franchise Tax Board. Those clients have been contacted directly and are receiving individualized assistance. If you are a client receiving this letter, we are notifying you because your information was stored in the affected system, and we want you to have the information you need to protect yourself.

**What Information was Involved**

The information potentially involved includes one or more of the following: Name, Social Security number, date of birth, address, employment information (such as employer name and wage information), phone number, and certain financial account information related to tax preparation (such as bank routing and account numbers used for direct deposit or payment of taxes).

At this time, aside from the limited number of clients for whom fraudulent returns were filed and who are being assisted in coordination with the IRS and California Franchise Tax Board, we have no evidence that the information of other clients has been misused.

**What We Are Doing.**

Upon discovery, we:

- Immediately secured the affected systems and engaged independent cybersecurity professionals to investigate and remediate the incident.
- Isolated and dismantled the affected computer to ensure it can no longer be used or accessed in our environment.
- Notified the Internal Revenue Service and the California Franchise Tax Board, who blocked the fraudulent returns from being processed and funded.
- Coordinated with these agencies so that the affected taxpayers will not incur out-of-pocket costs related to those fraudulent returns.
- Enhanced our security measures, including adding additional layers of security for access controls, additional monitoring, updating software and passwords, and retraining staff.

We have also notified appropriate regulatory authorities, as required by applicable law.

**What you can do**

Out of an abundance of caution, we recommend that all clients take the following steps to protect themselves from potential identity theft or tax-related fraud:

- **Consider an Identity Protection PIN (IP PIN).** The IRS offers an IP PIN program that can help prevent someone from filing a tax return using your Social Security number. You can learn more and enroll at www.irs.gov/ippin.

- **Monitor your tax records.** If you have not yet filed your tax return, consider filing it as soon as you reasonably can.
- **Set up and monitor your online tax accounts**. The IRS and California Franchise Tax Board recommend that taxpayers create and use secure online accounts to monitor their tax records and activity. You can create an IRS Online Account (which uses ID.me for identity verification) at: https://www.irs.gov/payments/online-account-for-individuals.
  You can create a MyFTB account to view and manage your California tax information at: https://www.ftb.ca.gov/online/myftb/index.asp.
- **Review notices from the IRS or state tax authorities.** Be alert for any letters indicating a return was filed in your name that you did not file, or that you received wages from an employer you do not recognize.
- **Monitor your accounts and credit reports.** Review bank, credit card, and other financial account statements regularly and check your credit reports for unfamiliar activity. You can obtain free credit reports at www.AnnualCreditReport.com or by calling 1-877-322-8228.
- **Place a fraud alert or credit freeze, if appropriate.** Contact any of the three major credit bureaus (Equifax, Experian, or TransUnion) to place a fraud alert or credit freeze on your file.
- **Watch for phishing attempts.** Be cautious of unsolicited calls, emails, or texts asking for personal or financial information, especially those referencing taxes or refunds.

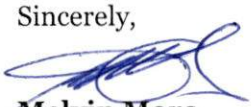
If you believe you are the victim of tax-related identity theft (for example, you receive notice that a tax return was filed using your Social Security number that you did not file), you should follow IRS guidance, which may include filing Form 14039, Identity Theft Affidavit, and contacting the IRS Identity Protection Specialized Unit.

**For more information**

We understand the severity of this incident and there are not enough words to express how deeply we regret this. While we are not perfect, we are fully committed to continue doing everything possible to make this right and to keep your confidence. **WE ARE HERE TO ASSIST YOU.** Contact you tax professional directly or the office if you have any questions, need assistance with any of the steps outlined in this letter, or would like to discuss your individual situation, please contact us at:

- Phone: [818-899-6404], Monday–Friday, [10 AM – 6 PM, PST]
- Email: [stephanie@melvinmora.com]
- Mailing address: [13618 Van Nuys Blvd. Pacoima CA 91331]

Sincerely,



**Melvin Mora,**

***President***

**Melvin Mora & Associates Inc**

13618 Van Nuys Blvd.

Pacoima CA 91331