

## DATA BREACH NOTIFICATION

April 26, 2025

### IMPORTANT NOTICE TO ALL CLIENTS

RE: DATA BREACH INCIDENT

Dear Clients:

We are contacting you about a data compromise that has occurred at Alfano Immigration Law, P.A. This notice provides details of the event and additional steps you can take to help protect your personal information.

**What Happened:** On April 3, 2025, an unauthorized user gained access to the Alfano Immigration Law, P.A. email and Dropbox accounts through a phishing attack. We became aware of the intrusion on Monday morning, April 7, 2025, and our IT service immediately acted, taking all impacted accounts offline and eliminating unauthorized access.

**What Information Was Involved:** After investigation, our IT experts found inconclusive evidence of exfiltration. Limited documents were contained within Dropbox and the unauthorized user did not gain access to our computer system files. At this time, our best information is any personal, non-public information shared via email could have been compromised. Personal information is generally defined as:

- a. **An individual's first name or initial and last name in combination with one or more of the following data elements for that individual:**
  - **A social security number;**
  - **A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;**

**What We Are Doing:** We take the privacy and security of personal information seriously and are working alongside our IT specialists to improve any vulnerabilities which may have contributed to this event.

**What You Can Do:** The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year. We strongly urge you to contact one of the agencies as soon as possible:

Equifax: [equifax.com/personal/credit-report-services](https://equifax.com/personal/credit-report-services) or 1-800-685-1111

Experian: [experian.com/help](https://experian.com/help) or 1-888-397-3742

TransUnion: [transunion.com/credit-help](https://transunion.com/credit-help) or 1-888-909-8872

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. Consumers have the right to order a free credit report from each of the three major credit reporting companies every year. These national credit bureaus have a centralized website, toll-free telephone number, and mailing address. This makes ordering easily and all in one place:

<https://www.annualcreditreport.com/index.action>. If your personal information has been misused, visit the FTC's site at [IdentityTheft.gov](https://www.ftc.gov/identitytheft) to report the identity theft and get recovery steps. *Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.*

There are also several free credit monitoring services:

Experian: <https://www.experian.com/credit/credit-monitoring/>

Credit Karma: <https://www.creditkarma.com/credit-monitoring>

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

**For More Information:** Please also visit the FTC's website, [IdentityTheft.gov/databreach](https://www.ftc.gov/identitytheft), about steps you can take to help protect yourself from identity theft. The steps are based on the types of information exposed in this breach.

Due to the size of this mailing, please understand that we may not be able to respond to telephone inquiries about the incident. We ask that you kindly forward any comments or questions in writing, and we will respond as quickly as possible.

We sincerely regret having to inform you of this incident and apologize for any inconvenience to you.

Sincerely,

Lea Alfano

Alfano Immigration Law, P.A.

This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message and are hereby notified that any disclosure, copying, or distribution of this message, or the taking of any action based on it, is strictly prohibited.

**Lea Alfano**

Alfano Immigration Law, P.A.

6900 Tavistock Lakes Blvd.

Suite 400

Orlando, FL 32827

T: (407) 307-4580

F: (407) 203-4848

[lea@alfanoimmigration.com](mailto:lea@alfanoimmigration.com)

Pronouns: (she/her/hers)

**NOTICE:** All non-U.S. citizens in the United States are required by regulation (8 CFR 265) to notify USCIS of any change in their address within 10 days of the change by filing Form AR-11 with the USCIS. Notifying the USCIS of any address change is a condition of a non-U.S. citizens' stay in the United States. Failure to comply could result in removal from the United States. Form AR-11 may be found online: <https://www.uscis.gov/ar-11>. You may mail your Form AR-11 to the address indicated on the bottom of the form or complete and submit Form AR-11 online: <https://egov.uscis.gov/coa/displayCOAForm.do>. Please also immediately notify our office of any change in address.