



Lindstrom CPA
4767 New Broad Street #1069
Orlando, FL 32814
Phone: 407-788-6898
Fax: 407-788-6545
info@lindstrom-cpa.com
www.lindstrom-cpa.com

[DATE]

[NAME]

[ADDRESS]

[CITY, STATE, ZIP]

Dear [NAME],

We are writing to inform you that Lindstrom Tax & Business Services, PLLC (“Lindstrom” or “we”) experienced a recent data incident (the “Incident”) that involved your personal information (“Information”). This letter provides you with information about this Incident, our response, and information on where to direct your questions. As a precaution, we have also provided steps you can take to protect your Information, including the ability to enroll in credit monitoring services that we are offering free of charge for twenty-four (24) months.

What Happened?

In May 2025, we learned that a limited number of potentially fraudulent tax returns had been filed using information of a limited number of our clients. Upon discovery, we began an investigation to determine whether these returns were related to any activity in our computer systems. As a result of our investigation, we identified suspicious activity in our network and immediately took steps to contain the situation, including isolating the affected user, changing passwords, notifying the Internal Revenue Service (“IRS”), working closely with representatives from our tax preparation software, deploying monitoring software, and engaging data security and privacy professionals to assist. The investigation determined that an unauthorized actor accessed files containing your Information as part of their attempt to file fraudulent tax returns and collect improper refunds from the federal government and state tax authorities. Besides this effort to defraud the government, we are not aware of any other misuse of information related to the Incident.

What Information Was Involved?

Our investigation has now determined that the following types of Information related to client tax files may have been impacted as a result of this Incident: name and social security number.

What We Are Doing.

Upon becoming aware of the Incident, we notified the IRS and have since worked closely with tax authorities to share information and take steps to protect our clients’ information. We have also added technical security protections on top of our existing protections by following the guidance of data security and privacy professionals and implementing additional technical safeguards. After determining unauthorized activity occurred on our systems, we immediately began analyzing the information involved to confirm the identities of potentially affected individuals and notify them.

What Can You Do?

To help protect your identity, we are offering complimentary access to Equifax Credit Watch Gold for twenty-four (24) months. To start monitoring your personal information, please follow the steps below.

Go to **www.equifax.com/activate**. Enter your unique activation code of [insert code] then click “Submit” and follow these four (4) steps:

1. **Register:** Complete the form with your contact information and click “Continue”.
If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:** Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click ‘Sign Me Up’ to finish enrolling.

The confirmation page shows your completed enrollment. Click “View My Product” to access the product features. You must enroll by December 31, 2025 (Your code will not work after this date).

Additionally, it is always recommended that you remain vigilant, regularly monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Please also review the “Additional Resources” section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have any questions, you may call us at (407) 788-6898 Monday through Thursday from 9:00 am to 5:00 pm and Friday from 9:00 am to 3 pm Eastern Time (excluding U.S. holidays).

Sincerely,

A handwritten signature in black ink, appearing to read 'Tiffani Lindstrom CPA', with a stylized flourish at the end.

Tiffani Lindstrom, CPA
Lindstrom CPA

Encl.

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Massachusetts residents: You may obtain one (1) or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. 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.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Massachusetts Residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. You have the right to obtain a police report if you are a victim of identity theft.

How to Apply for an IRS Identity Protection PIN

- Go to: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.
- Select the button: “Get an IP PIN.”
- The fastest way to receive an IP PIN is to request one through your ID.me account, under your “Profile” page. If you don’t already have an account on IRS.gov, you must register to validate your identity.
- Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process.
- Once you have opted in and obtained an IP PIN online, you will need to retrieve your IP PIN online each calendar year as a CP01A Notice will not be mailed. The IP PIN is generally available in your online account starting in mid-January through mid-November.

If you need help applying for this PIN, please call our office.

The IRS offers a sign-in option with ID.me, which offers access to IRS online services with a secure account that protects your privacy.

ID.me is an account created, maintained, and secured by a technology provider.

If you don't have an ID.me account, you must create a new account.

Sign in with an existing account

Sign in with **ID.me**

OR

Create a new account

ID.me Create an account