Ernst & Young LLP
One Manhattan West (395 9th Avenue)
New York, NY 10001

July 13, 2026

NOTICE OF DATA BREACH

SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A. Sample,

Ernst & Young LLP ("EY" or "we") is writing to inform you of a data security incident that involved your personal information. EY provides professional tax services to a wide range of financial institutions globally. In the course of providing these tax services, EY received certain personal information relating to your investment holdings with [EY CUSTOMER]. EY is committed to protecting your personal information, which is why we are writing to explain what happened, what information was involved, our response, and the resources available to help you further protect your personal information.

What Happened?

EY uses a third-party information technology service management platform to help EY information technology personnel provide support to EY teams performing tax-related work for clients. Support tickets submitted through the platform may include documents containing client tax information. On April 23, 2026, EY identified anomalous activity within that platform. EY's Information Security team immediately initiated its incident response procedure to determine the nature and scope of the incident, contain it, and begin remediation and recovery efforts. EY has worked with an independent cybersecurity firm to investigate the incident and confirm that the unauthorized access has been stopped, and our systems are now secure.

Based on EY's investigation and available evidence, between March 28, 2026, and April 12, 2026, an unauthorized third party accessed the platform referenced above and downloaded documents pertaining to a number of EY clients.

What Information Was Involved?

Your personal information affected by this incident includes the following: [DATA ELEMENTS], and certain financial information contained in or used to prepare tax filings.

At this time, we are not aware of any misuse or further exposure of your personal information as a result of this incident. Further, we do not have any indication your personal information was specifically targeted. Nevertheless, we are providing information about steps you can take to further secure your personal information.

What We Are Doing.

We take the confidentiality, privacy, and security of your information seriously. Upon discovery, we took steps to secure our systems and launched an investigation with third-party specialists to determine the nature and scope of the event, and additionally notified federal law enforcement of this incident. We continue to monitor for further information associated with this incident, including monitoring for information that was exposed as a result of the incident.

To help protect your identity, we are offering complimentary access to two products offered by Experian: IdentityWorks, a credit and identity monitoring service, and Identity Restoration. To activate the credit and identity monitoring services available through Experian IdentityWorks as a complimentary 24-month membership, please follow the steps below:

- Ensure that you **enroll by 11:59 p.m. UTC** October 31, 2026 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit3b.
- Provide your **activation code**: ABCDEFGHI

Identity Restoration is a service that may be used to help resolve fraudulent identity theft if you believe you were victim of identity theft. Please note that Identity Restoration is available from the date of this letter and does not require any action on your part at this time as this service is provided to you regardless of enrollment in IdentityWorks. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. To use Identity Restoration, if you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent, at the number provided below. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent will work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

If you have questions about Experian IdentityWorks, or would like to enroll by phone, please contact Experian's customer care team at 833-931-7884 by October 31, 2026 and Experian's customer care team can assist you.

Be prepared to provide activation code [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and you will have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and TransUnion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available, regardless of your enrollment in IdentityWorks, to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do.

In addition to utilizing the credit and identity monitoring services described above, EY recommends that you remain vigilant against incidents of identity theft and fraud and carefully review your online and financial accounts for any suspicious activity.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account and promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to the proper law enforcement authority.

Anyone who has an SSN or individual taxpayer identification number (ITIN) and is able to verify his/her identity is eligible to enroll into the IP PIN program. The identity protection PIN (IP PIN) is a six-digit number that prevents someone else from filing a tax return using your Social Security number (SSN) or individual taxpayer identification number (ITIN). The IP PIN is known only to you and the IRS. It helps us verify your identity when you file your electronic or paper tax return. If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft, even if you are not required to file a tax return. More information regarding requesting an IP PIN can be found on the IRS's website at https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

EY is providing additional information below about steps you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report if you choose to do so.

For More Information.

We understand that you may have questions or may seek additional information. If you have additional questions, please call us at 833-931-7884 from Monday – Friday (excluding major U.S. holidays) 8 a.m.– 8 p.m. CST email us at Privacy.Notification@ey.com.

Sincerely,

Robb J Canning
Deputy Ethics and Compliance Officer
Ernst & Young LLP

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Steps You Can Take to Protect Against Identity Theft and Fraud

Order Credit Report

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Place A Fraud Alert

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

	Experian	Equifax	TransUnion
Phone	1-888-397-3742	1-888-836-6351	1-800-916-8800
Address	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	Equifax Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374	TransUnion LLC P.O. Box 1000 Chester, PA 19016
Online Credit Report Fraud Alert Form	https://www.experian.com/help/fraud-alert/	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts	https://www.transunion.com/fraud-alerts

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.

Place A Security Freeze

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all your credit files. To find out more on how to place a security freeze, you can use the following contact information:

	Experian	Equifax	TransUnion

Phone	1-888-397-3742	1-888-298-0045	1-800-916-8800
Address	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	https://www.experian.com/help/credit-freeze/	https://www.equifax.com/personal/credit-report-services/credit-freeze/	https://www.transunion.com/credit-freeze

To request a security freeze, you will need to provide some or all the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security Number
3. Date of Birth
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. Social Security Card, pay stub, or W2
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, via their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that 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, your state Attorney General, or the Federal Trade Commission. This notice has not been delayed by law enforcement.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You can learn more about how to protect yourself against identity theft by visiting www.usa.gov/identity-theft and www.ftc.gov/idtheft.

Maryland Residents: You may obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft at: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; Telephone: 1-888-743-0023; https://oag.maryland.gov/i-need-to/Pages/identity-theft-information.aspx.

New York Residents: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General Consumer Frauds & Protection Bureau 120 Broadway, 3rd Floor New York, NY 10271 (800) 771-7755 www.ag.ny.gov	New York Department of State Division of Consumer Protection 99 Washington Avenue, Suite 650 Albany, NY 12231 (800) 697-1220 www.dos.ny.gov

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office at: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001; Telephone: 1-919-716-6400; www.ncdoj.gov.

Oregon Residents: We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 or 1-503-378-4400; www.doj.state.or.us.

Washington D.C. Residents: You can obtain additional information about the steps you can take to avoid identity theft from the DC Office of the Attorney General at https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft. You may also contact the DC Office of the Attorney General at 400 6th Street NW, Washington, D.C. 20001; (202) 727-3400; and oag@dc.gov.

New Mexico residents: Consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_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.

Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov. As of the date of this mailing, the approximate total number of Rhode Island residents receiving notification of this incident is 7.

Vermont Residents: Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at https://ago.vermont.gov/

All U.S. Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.