

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

ERNEST F. KOSCHINEG, ESQ.
ekoschineg@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

October 27, 2022

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Barry J. Kay & Co., CPAs ("Kay") located at 98 Cuttermill Road, Suite 335-S, Great Neck, New York 11021 and write to inform you of a recent data security incident. By providing this notice, Kay does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On September 21, 2022, Kay became aware that certain client 2019 tax returns were subject to unauthorized access. Kay was made aware of this unauthorized access via a compromised file listing provided by the FBI. The FBI advised that likely in early 2020, Kay was the victim of a phishing campaign which had been targeting tax and accounting firms in the tri-state area. The phishing email would have contained an attachment which, upon clicking, would have launched malware, allowing for unauthorized access to Kay's systems. Neither Kay nor the FBI is aware of any fraudulent filings or misuse of information found in the compromised files. Upon discovery, Kay immediately reviewed the list of impacted files and retained third party specialists to assist with its response to this incident. Because the compromised files were tax documents that contained sensitive client information, Kay then compiled a list of clients potentially impacted and worked to obtain sufficient address information in order to provide notification. On October 10, 2022, that process was completed, and it was determined that information related to 2 Maryland residents was potentially subject to unauthorized access. The information contained in the tax returns would have included first and last name, in combination with a Social Security number and bank account information.

On October 26, 2022, Kay sent written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to individuals is substantially similar to the letter attached hereto as Exhibit "A."

Very truly yours,



Ernest F. Koschineg
CIPRIANI & WERNER, P.C.

Exhibit A

BARRY J. KAY & CO.

Certified Public Accountants

Barry J. Kay C.P.A.

Jerome J. Giorlando C.P.A.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(NOTICE OF DATA BREACH - CA Residents)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a data security incident experienced by Barry J. Kay & Co., CPAs that may have involved your information described below. While we have no evidence of attempted or actual misuse of your information as a result of this incident, out of an abundance of caution, we are providing you with information about the incident, our response, and steps you can take to help protect your information.

What Happened: On September 21, 2022, Barry J. Kay & Co., CPAs became aware that certain client 2019 tax returns were subject to unauthorized access. Upon discovery, we immediately began working with third-party specialists to conduct an investigation to determine how this occurred, and to understand the full nature and scope of this incident. We are also working with federal law enforcement. Because there was unauthorized access to personal information contained within the tax returns, we then compiled a list of clients potentially impacted and worked to obtain sufficient address information in order to provide notification. That process was completed on October 10, 2022. We are now notifying potentially impacted individuals out of an abundance of caution.

What Information Was Involved: The personal information believed to potentially be at risk, includes your first and last name, in combination with your Social Security number. Additionally, your financial information may be at risk if you provided your bank account information in connection with receiving your tax return funds via direct deposit, or if you paid your taxes via direct debit.

What We Are Doing: Upon discovery, we immediately engaged third-party specialists to investigate this matter and assist with our response. Out of an abundance of caution, we have arranged for you to activate, at no cost to you, identity monitoring services for 12 months provided by Kroll. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary identity monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

What You Can Do: We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can activate the complimentary credit monitoring service we are making available to you. You can also review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at (855) 532-1782, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays.

We take the privacy and security of the information in our care seriously, and sincerely regret any worry or inconvenience this incident may cause you and your family.

Sincerely,

A handwritten signature in cursive script that reads "Barry Kay".A handwritten signature in cursive script that reads "Jerome J. Giorlando".

Barry J. Kay, CPA and Jerome J. Giorlando, CPA

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until **<<b2b_text_6(activation deadline)>>** to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;

4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com	Experian 1-888-397-3742 www.experian.com	Equifax 1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Barry J. Kay & Co., CPAs may be contacted at 98 Cuttermill Road, Suite 335-S, Great Neck, NY 11021.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>. Barry J. Kay & Co., CPAs may be contacted at 98 Cuttermill Road, Suite 335-S, Great Neck, NY 11021.