

Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

June 27, 2022

Via Online Submission

Attorney General Aaron Fey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

To Whom It May Concern:

We represent Ferguson Private Wealth Management (“Ferguson”) with respect to a data security incident involving potential exposure of certain personally identifiable information (“PII”) described in more detail below. Ferguson is a financial planning group in Lansdowne, Virginia. Ferguson is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

In October 2021, during an internal audit, Ferguson determined that suspicious activity associated with its email environment in October 2020 required further review. This review determined that there was unauthorized access to two email accounts, however the investigation was unable to determine the time period for any unauthorized access. Ferguson then hired a third-party to review the contents of the accounts to determine whether any personal information was stored in the accounts. This review was completed on May 2, 2022, at which point it was determined that personal information for some clients was present in the account. Potentially affected information may include clients first and last names, addresses, dates of birth, driver’s license numbers, Social Security numbers, financial information, and for a small subset of individuals, health insurance policy number, and limited health information, which may include provider name, diagnosis or treatment information, or medication.

2. Number of residents affected.

One (1) Maine resident may have been affected and was notified of the incident. A notification letter was sent to the potentially affected individual on June 24, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

June 27, 2022

Page 2

3. Steps taken in response to the incident.

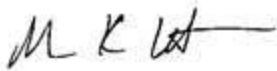
Ferguson took steps to address this incident and to prevent similar incidents in the future, including changing all passwords, deploying multi-factor authentication for remote access, and retraining staff on recognizing and responding to suspicious computer activity. Affected individuals were offered 12 months of credit monitoring and identity protection services from Kroll, LLC.

4. Contact information.

Ferguson takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read 'M K Ventrone', with a horizontal line extending to the right.

Melissa K. Ventrone
Member

FERGUSON

PRIVATE WEALTH MANAGEMENT

<<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 Security [Incident / Breach])>>

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

I hope this letter finds you well and that you are enjoying your spring and looking forward to summer. At Ferguson Private Wealth Management (“Ferguson PWM”), we value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may have impacted your personal information. This letter contains details regarding the incident, and resources we are making available to help you better protect your personal information.

What happened:

In October 2021, during an internal audit, we determined that suspicious activity associated with our email environment in October 2020 required further review. This review determined that there was unauthorized access to two email accounts. We then hired a third-party to review the contents of the accounts to determine whether any personal information was stored in the accounts. This review was completed on May 2, 2022, at which point we determined that your personal information was present in the account.

What information was involved:

Information present in the email accounts may include your <<b2b_text_2 (“first and last name,” and data elements)>>.

What we are doing:

We have taken steps in response to this incident to enhance the security of our email environment, including changing all passwords and deploying multi-factor authentication for remote access. We have also arranged for you to receive identity monitoring services from Kroll for 12 months at no cost to you, including Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

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

You have until <<b2b_text_6 (date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What you can do:

It is always a good idea to remain vigilant for incidents of identity theft or fraud, and to review your bank account and other financial statements as well as your credit reports for suspicious activity. We also encourage you to contact Kroll with any questions and to take full advantage of the Kroll service offering. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information:

If you have any questions or concerns, please call [TFN] Monday through Friday from 8 am – 5:30 pm Central Time, excluding some U.S. holidays. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,



John Ferguson

President

Ferguson Private Wealth Management

Securities offered through Registered Representatives of Cambridge Investment Research, Inc. A Broker/dealer, Member FINRA/SIPC. Advisory offered through CIRA a Registered Investment Advisor. Ferguson Private Wealth Management and Cambridge are not affiliated.



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.

WEB WATCHER

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

PUBLIC PERSONA

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

QUICK CASH SCAN

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 MILLION IDENTITY FRAUD LOSS REIMBURSEMENT

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

FRAUD CONSULTATION

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to 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.

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order 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 or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

Experian Fraud Reporting and Credit Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

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.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.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.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. [A total of \[XX\] Rhode Island residents were notified of this incident.](#)

All US 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.