

Jason M. Schwent
T (312) 985-5939
F (312) 517-7573
Email: jschwent@ClarkHill.com

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

March 8, 2022

Via USPS

Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

We represent Douglass Financial Services ("Douglass Financial") with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. Douglass Financial is an independently owned financial consulting firm servicing clients in Bloomington, Illinois. Douglass Financial 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.

On September 29, 2021, Douglass Financial became aware of suspicious activity associated with one of its corporate email accounts. Douglass Financial immediately began an internal investigation and hired a third-party vendor to conduct an in-depth review of the email account to determine what personal information may have been located in the account and to extract contact information of potentially affected individuals. This review was completed on January 28, 2022. From this review, it appears the information in the account may have included individual's names and physical address in combination with one or more of the following data elements: name, address, Social Security number, date of birth, and driver's license number or state identification number.

2. Number of residents affected.

One (1) Maryland residents may have been affected and was notified of the incident. A notification letter was sent to the potentially affected individual on March 8, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

March 8, 2022

Page 2

3. Steps taken in response to the incident.

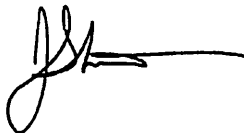
Douglass Financial took steps to address this incident and prevent similar incidents in the future. Douglass Financial changed the passwords to the affected corporate email account and multifactor authentication was enabled across all Douglass Financial corporate email accounts. Additionally, affected individuals were offered 12 months of credit monitoring and identity protection services through Kroll.

4. Contact information.

Douglass Financial takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read 'JS', followed by a horizontal line extending to the right.

Jason M. Schwent
Senior Counsel

cc: Mariah Leffingwell – mleffingwell@clarkhill.com



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

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

<<b2b_text_4(SubjectLine)>>

Dear <<First_Name>> <<Last_Name>>,

Douglass Financial Services ("Douglass Financial") recently experienced a data security incident that may have impacted some of your personal information. Douglass Financial is an independently owned financial consulting firm serving clients in Central Illinois. Douglass Financial takes the privacy and security of your information seriously, and sincerely apologizes for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What happened?

On September 29, 2021 we learned of suspicious activity associated with one of our corporate email accounts. As soon as we learned of the incident, we began an internal investigation and hired a third-party vendor to conduct an in-depth review of the email account to determine what personal information may have been located in the account, and to extract contact information of potentially affected individuals. This review was completed on January 28, 2022, at which point we identified that some of your personal information may have been located in the corporate email account at issue. While we have no indication that any of your personal information has been misused, out of an abundance of caution, we wanted to notify you about this incident and provide you with resources to help protect yourself.

What information was involved?

From the review, it appears that your <<b2b_text_1(DataElements)>><<b2b_text_2(DataElements)>><<b2b_text_3(DataElements)>> may have been impacted by this incident.

What we are doing?

Although we do not believe there is any risk that your information will be misused, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. 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. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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

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

Membership Number: <<MembershipNumber (S_N)>>

More information describing your services is included with this letter.

We want to assure you that we have taken steps to prevent this kind of event from happening in the future. Since the incident, the password to the affected corporate email account was changed and multifactor authentication was enabled across all Douglass Financial corporate email accounts.

What you can do:

We encourage you to remain vigilant against incidents of identity theft by reviewing your bank account and other financial statements as well as your credit reports for suspicious activity.

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

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

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.

Please review the enclosed "Recommended Steps" section included with this letter. This section describes additional steps you can take to help protect yourself, 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 1-855-541-3553 Monday through Friday from 8 am – 5:30 pm Central Time, excluding major U.S. holidays. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Douglass Financial Services

* Securities offered through Registered Representatives of Cambridge Investment Research, Inc. A broker/dealer, Member FINRA/SIPC. Advisory Services offered through Cambridge Investment Research Inc., a Registered Investment Advisor. Douglass Financial Services and Cambridge are not affiliated.

Recommended Steps to Help Protect Your Information

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

1. 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 can help you determine if it's an indicator of identity theft.

2. Fraud Consultation. You have unlimited access to consultation with a Kroll 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.

3. 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

4. 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.

5. Place Fraud Alerts. We recommend you 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.

6. 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.

7. **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/201904_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.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft