Clark Hill

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

April 1, 2022

Sent via USPS

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

Dear Attorney General Brian E. Frosh

We represent Duncan Disability Law, S.C. ("DDL") with respect to a data security incident involving potential exposure of certain personally identifiable information ("PII") described in more detail below. DDL is a law firm that represents individuals in social security and workers compensation disputes. DDL 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 November 11, 2021, DDL discovered a security incident impacting its systems. As soon as DDL learned about the incident, they began an internal investigation to determine what occurred and whether any personal information was compromised. The investigation determined that an unauthorized actor gained access to some of DDL's systems and deployed malware in the environment.

DDL was unable to determine which, if any, sensitive information was accessed, and out of an abundance of caution decided to notify all clients whose personal information was stored on its systems at the time of this incident. The sensitive information stored on the system at the time of the incident includes names, Social Security numbers, date of birth, birth certificates, addresses, and mother's maiden name.

2. Number of residents affected.

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

3. Steps taken in response to the incident.

DDL took steps to address this incident and to prevent similar incidents in the future, including changing all system and user passwords and monitoring email environments for suspicious activity, in addition to other measures. Affected individuals were offered 12 months of credit monitoring and identity protection services through IDX.

4. Contact information.

DDL takes the security of their client's information very 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 mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL

M K Vt

Melissa K. Ventrone
Member

Exhibit A

Duncan Disability Law, S.C.
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-774-1219
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 1, 2022

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

Duncan Disability Law, S.C. ("DDL") recently experienced a data security incident that may have impacted your personal information. DDL may have received your information as part of the provision of legal services to you. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. We wanted to provide you with details regarding this incident, and resources we are making available to you.

What Happened?

On November 11, 2021, DDL discovered a security incident impacting our systems. As soon as we learned about the incident, we began an internal investigation to determine what occurred and whether any personal information was compromised. Our investigation determined that an unauthorized actor gained access to some of our systems and deployed malware in the environment. We wanted to let you know about this incident out an abundance of caution because your information may have been stored on these systems.

What Information Was Involved?

Information stored in our system may contain your name, Social Security number, date of birth, birth certificate, address, and mother's maiden name.

What We Are Doing:

We are taking steps in response to this incident to enhance the security of our systems, including changing all passwords, implementing multifactor authentication, installing endpoint monitoring software, and other security controls.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 / 24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To receive credit monitoring services, you must be over the age of 18, 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 information describing these 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 encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-774-1219 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 1, 2022.

Additional information about protecting your identity is available 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

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-774-1219 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have. Your trust is our top priority, and we deeply regret any inconvenience or concern that this may cause you.

Sincerely,

Dana Duncan

Dana Duncan, Esq.
Duncan Disability Law, S.C.

IDX The Privacy Platform

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-774-1219 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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 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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	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.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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.

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.