

16058

EXHIBIT A

November 15, 2019

Notice of Data Breach

Dear _____,

You are receiving this notification because Friedman Law Group Ltd. ("FLG") recently had a security incident. An unauthorized individual gained access to the email account of FLG's former employee by way of a phishing email, and this unauthorized individual gained access to your personally identifiable information.

What Happened?

On October 16, 2019, an FLG employee received an email from a client requesting login information; FLG's client's email had been compromised by a hacker, although FLG was not aware of this at the time.

The FLG employee clicked this link, not knowing the client's email account was compromised, and entered her FLG username and password. An unauthorized person then used these credentials to log into the employee's email account, and this person downloaded a copy of the email account at this time. After the download, on October 17, 2019, an unauthorized person then used the FLG account to send out a variety of spam emails.

The unauthorized access was detected and terminated on October 17, 2019, and law enforcement was notified of the breach. This notification was not delayed as a result of a law enforcement investigation.

What Information Was Involved?

The email account of FLG's now former employee, who served as FLG's primary project and office administrator, was compromised. This email account contained emails and attachments that contained names, social security numbers, addresses, photographs of identity documentation, phone numbers, and other personally identifiable information for approximately 38 individuals, primarily contained in W-2, W-4, W-9, and other such documents, as well as other personally identifiable information that varies by the individual affected. You are receiving this notice because our review located emails or attachments that contained your personally identifiable information.

What We Are Doing.

We have searched and reviewed the compromised account to determine which emails and attachments in the compromised email account contain personally identifiable information requiring legal notification to individuals under applicable law.

We have also undertaken a multitude of steps to strengthen data security at FLG and to ensure that there is no further unauthorized access to FLG's information systems. We take information security and confidentiality seriously and apologize for any inconvenience.

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by **February 28, 2020** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: _____

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by **February 28, 2020**. Be prepared to provide engagement number DB16466 as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 12-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 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. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available 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.
- **Up to \$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers. 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.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (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).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration; you will also find self-help tips and information about identity protection at this site.

What You Can Do.

We encourage you to utilize the provided, pre-paid, no charge to you identity theft prevention and mitigation services from Experian, described above.

For residents of Maryland, please note that the following contact information for the Office of the Maryland Attorney General may be used to obtain additional information about how to avoid identity theft. The attorney general's office may be reached, toll-free, at 1-888-743-0023. You may also visit the Office of the Maryland Attorney General at the address below or online at the website below.

Brian E. Frosh, Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

<http://www.marylandattorneygeneral.gov/>

<http://www.riag.ri.gov/index.php>

For residents of Wisconsin, please note that we have identified and know of the acquisition of personal information pertaining to you, and upon your written request to the contact information provided in this letter,

FLG will identify the personal information pertaining to you that was accessed and acquired by the unauthorized party mentioned above.

For More Information.

For more information, you may call us at 773.248.9455 or write us at afriedman@marketing-law.com.

We apologize for any inconvenience this may have caused you.

Sincerely,

Andrea E. Friedman, Esq.
Friedman Law Group, Ltd.
afriedman@marketing-law.com
773.248.9455

How to Further Protect My Information.

State law allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any request you make for new loans, credit, credit or debit cards, mortgages, employment, housing or other services.

If at any time you become a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze.

Credit Report Security Freeze Instructions

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-525-6285

TransUnion Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
1-800-680-7289

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-800-349-9960

In order to request a security freeze, you will need to provide the following information:

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, provide the addresses where you have lived over the prior five years;

5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, a payment of \$5.00 by check, money order, or credit card (Visa, MasterCard, American Express or Discover only) for the freeze. Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. 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.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (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 or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Identity Theft — FTC Contact Information

The Federal Trade Commission is located at 600 Pennsylvania Avenue, NW Washington, DC 20580. If you believe you may have been a victim of identity theft, you may file a complaint with the Federal Trade Commission at: www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338).

Here are a few warning signs to help you determine that whether your personal information may have been used by someone else:

- Receiving a bill for services you did not purchase or receive never used
- Being contacted by a debt collector about debt you do not owe
- Seeing collection notices on your credit report that you do not recognize

If you believe someone else may have used your information, you may wish to consider taking additional steps which are outlined on the Federal Trade Commission's website at www.ftc.gov