

December 12, 2022

**Anjali C. Das**  
312.821.6164 (direct)  
Anjali.Das@wilsonelser.com

**Via Online Portal:**

**Attorney General Aaron Frey**  
Office of the Attorney General  
Attn: Security Breach Notification  
Department of Professional & Financial Regulation  
Bureau of Consumer Credit Protection  
35 State House Station  
Augusta, Maine 04333

**Re: Cybersecurity Incident Involving The Haggard Law Firm, P.A.**

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents The Haggard Law Firm, P.A. (“Haggard”), a personal injury law firm located at 330 Alhambra Circle, Coral Gables, Florida 33134, with respect to a cybersecurity incident that was first discovered by Haggard in November, 2021 (hereinafter, the “Incident”). Haggard takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of residents being notified, and the steps that Haggard has taken in response to the Incident. We have also enclosed hereto a sample of the notification to be made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

**1. Nature of the Incident**

Haggard Law Firm (“Haggard”) was alerted to suspicious activity by a third party in November 2021 suggesting a potential business email compromise. Haggard proceeded to conduct an internal investigation and discovered that an unauthorized party may have gained access to a single employee’s business email account. Thereafter, Haggard engaged a third party cybersecurity firm to conduct a forensics investigation to determine the nature and scope of the incident. The forensics investigation concluded on December 14th, 2021. Thereafter, Haggard engaged a third party vendor to mine the contents of the compromised account to identify those individuals whose information may have been impacted in addition to the type of personally identifiable information stored in the account. This process took time from February to September 2022. Once Haggard was able to verify the names and addresses of potentially impacted individuals, it proceeded to engage a notice vendor to assist with mailing the notice letters to individuals, setting up a call

---

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston  
Indiana • Kentucky • Los Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans  
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

[wilsonelser.com](http://wilsonelser.com)

center, and providing credit monitoring and identity theft protection services. At this time, Haggard is not aware of any individual's information that was misused. Nonetheless, Haggard is notifying all potentially impacted individuals out of an abundance of caution.

Although Haggard is unaware of any fraudulent misuse of information, it is possible that individuals' full name, and Driver's License may have been exposed as a result of this unauthorized activity.

As of this writing, Haggard has not received any reports of related identity theft since the date of the incident (November, 2021 to present).

## **2. Number of Maine residents affected.**

A total of one (1) Maine resident may have been potentially affected by this incident. A notification letter to this individual was mailed on December 12, 2022, by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

## **3. Steps taken in response to the Incident.**

Haggard is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, Haggard moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, Haggard engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, Haggard reset company passwords; implemented regular password changes; effected additional technical security measures; implemented Multi-Factor Authentication; employed more aggressive email filtering; conducted security awareness training; and took steps and will continue to take steps to mitigate the risk of future harm.

Although Haggard is not aware of any actual or attempted misuse of the affected personal information, Haggard is offering twelve (12) months of complimentary credit monitoring and identity theft restoration services through CyberScout to all individuals to help protect their identity. Additionally, Haggard will provide guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

## **4. Contact information**

Haggard remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at [Anjali.Das@WilsonElser.com](mailto:Anjali.Das@WilsonElser.com) or 312-821-6164.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**



Anjali C. Das

# **EXHIBIT A**

The Haggard Law Firm  
P.O. Box 3923  
Syracuse, NY 13220



[REDACTED]

December 12, 2022

### **Notice of Data Security Incident**

Dear [REDACTED],

We are writing to inform you of a data security incident which affected The Haggard Law Firm, P.A. (“Haggard”), a personal injury law firm operating in the Coral Gables, Florida area. The data security incident may have resulted in the potential compromise of some of your personal data. While we have no indication that your information has been misused, this letter contains information about the incident and information about how to protect your personal information going forward. Haggard considers the protection of sensitive information a top priority, and sincerely apologizes for any inconvenience as a result of the incident.

#### **What Happened**

Haggard Law Firm (“Haggard”) was alerted to suspicious activity by a third party in November, 2021 suggesting a potential business email compromise. Haggard proceeded to conduct an internal investigation and discovered that an unauthorized party may have gained access to a single employee’s business email account. Thereafter, Haggard engaged a third party cybersecurity firm to conduct a forensics investigation to determine the nature and scope of the incident. The forensics investigation concluded on December 14th, 2021. Thereafter, Haggard engaged a third party vendor to mine the contents of the compromised account to identify those individuals whose information may have been impacted in addition to the type of personally identifiable information stored in the account. This process took time from February to September 2022. Once Haggard was able to verify the names and addresses of potentially impacted individuals, it proceeded to engage a notice vendor to assist with mailing the notice letters to individuals, setting up a call center, and providing credit monitoring and identity theft protection services. At this time, Haggard is not aware of any individual’s information that was misused. Nonetheless, Haggard is notifying all potentially impacted individuals out of an abundance of caution.

#### **What Information Was Involved**

While we have no reason to believe that your information has been misused as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the unauthorized party may have had access to your: [REDACTED].

### **What We Are Doing**

The security and privacy of information contained within Haggard's systems is a top priority, and Haggard is taking additional measures to protect this information. Since the incident, Haggard has continued to strengthen its security posture by adding the following security controls: Haggard reset company passwords; implemented regular password changes; effected additional technical security measures; implemented Multi-Factor Authentication; employed more aggressive email filtering; conducted security awareness training; and took steps and will continue to take steps to mitigate the risk of future harm.

### **In response to the incident, we are providing you with access to the following services:**

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern Time, Monday through Friday. Please call the help line [REDACTED] and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

Additionally, we are providing you with access to **Single Bureau Credit Monitoring** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/haggard> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

### **What You Can Do**

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file.

Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause. If you have any questions, please do not hesitate to call [REDACTED] between the hours of 8:00 am to 8:00 pm Eastern Time, Monday through Friday.

Sincerely,

The Haggard Law Firm

## Steps You Can Take to Help Protect Your Information

**Credit Reports:** You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone or online. 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

### Experian

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

### TransUnion

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289

[www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

### Equifax

P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

**Monitoring:** You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

**Security Freeze:** You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

### Experian

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

### TransUnion

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

### Equifax

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

**File Police Report:** You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**FTC and Attorneys General:** You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

**For residents of Iowa:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

---

**For residents of Massachusetts:** It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

---

**For residents of New Mexico:** State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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.

---

**For residents of Oregon:** State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

---

**For residents of Rhode Island:** It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

---

**For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:** You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**Federal Trade Commission - Consumer Response Center:** 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); [www.identitytheft.gov](http://www.identitytheft.gov)

**Arizona Office of the Attorney General** Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

**Colorado Office of the Attorney General** Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 [www.coag.gov](http://www.coag.gov)

**District of Columbia Office of the Attorney General** – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; [www.oag.dc.gov](http://www.oag.dc.gov)

**Illinois office of the Attorney General** - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; [www.illinoisattorneygeneral.gov](http://www.illinoisattorneygeneral.gov)

**Maryland Office of the Attorney General** - Consumer Protection Division: 200 St. Paul Place, 16<sup>th</sup> floor, Baltimore, MD 21202; 1-888-743-0023; [www.oag.state.md.us](http://www.oag.state.md.us)

**New York Office of Attorney General** - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

**North Carolina Office of the Attorney General** - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; [www.ncdoj.com](http://www.ncdoj.com)

**Rhode Island Office of the Attorney General** - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; [www.riag.ri.gov](http://www.riag.ri.gov)

---