James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

August 19, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent the FireKing Security Group, LLC ("FireKing"), located at 101 Security Parkway, New Albany, IN 47150. We are writing to notify your office of an incident that may affect the security of personal information relating to one (1) New Hampshire resident. The investigation into this event is ongoing, and this notice may be supplemented if significant new facts are learned subsequent to its submission. By providing this notice, FireKing does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On May 15, 2019, FireKing determined there had been unauthorized access to certain FireKing employees' email accounts. FireKing first identified suspicious activity within the email accounts on April 3, 2019, and immediately launched an investigation, with the support of third-party forensic experts, into the nature and scope of the incident, the information that may have been improperly accessed, and the identities of the impacted individuals. FireKing also took steps to secure the email accounts. The investigation determined that an unauthorized party was able to access two employees' email accounts for various periods of time between February 18, 2019, and April 3, 2019. On or around June 26, 2019, FireKing confirmed the identities of the individuals who may have had information affected by this incident.

The personal information impacted by this event may include the following: name, address, payment card number, expiration date, and CVV.

Notice to New Hampshire Resident

On August 19, 2019 FireKing began providing written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the potential unauthorized access to the email accounts, FireKing moved quickly to identify those that may be affected, put in place resources to assist them, and provide them with notice of this incident. FireKing is also working to implement additional safeguards to protect the security of information in its system.

FireKing is providing written notice to those individuals who may be affected by this incident, including the contact information for a dedicated assistance line for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, FireKing is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. FireKing is also providing written notice of this incident to other state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4798.

Very truly yours,

James E. Prendergast of
MULLEN COUGHLIN LLC

JEP:plm
Enclosure

EXHIBIT A

FireKing
SECURITY GROUP
P.O. Box 589
Claysburg, PA 16625-0589

[redacted]

E8174-L03-0000002
SAMPLE A SAMPLE - STANDARD INDIVUDAL NOTICE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data Breach

Dear Sample A Sample:

The FireKing Security Group, LLC ("FireKing"), is writing to inform you of a recent event that may impact the privacy of some of your personal information. While we are unaware of any fraudulent misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On May 15, 2019, FireKing determined there had been unauthorized access to certain FireKing employees' email accounts. FireKing first identified suspicious activity within the email accounts on April 3, 2019, and immediately launched an investigation, with the support of third-party forensic experts, into the nature and scope of the incident, the information that may have been improperly accessed, and the identities of the impacted individuals. FireKing also took steps to secure the email accounts. The investigation determined that an unauthorized party was able to access two employees' email accounts for various periods of time between February18, 2019, and April 3, 2019.

What Information Was Involved? On June 26, 2019, we determined an email message containing the following types of information relating to you was accessible to the unknown actor during this incident: exposed element 1, exposed element 2, exposed element 3, exposed element 4, exposed element 5, and exposed element 6. To date, we have not received any reports of the misuse of your information.

What We Are Doing. Upon learning of this incident, we immediately took steps to secure the affected email accounts. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems to ensure the high priority we place on maintaining the privacy and security of information in our care is met. We also notified state regulators, as required.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Prevent Fraud and Identity Theft*. We encourage you to remain vigilant against incidents of identity theft by reviewing your account statements regularly and keep a close eye on your credit card activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of their credit report.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 812-542-3480, Monday through Friday during the hours of 8:00 a.m. to 5:00 p.m., Eastern Time. You may also write to FireKing Security Group at 101 Security Parkway, New Albany, IN 47150.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

Michael Lynch

Michael Lynch
Chief Financial Officer
FireKing Security Group, LLC

STEPS YOU CAN TAKE TO PREVENT IDENTIY THEFT AND FRAUD

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 activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

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 a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

To monitor for actual or attempted misuse of Social Security benefits, you can create an account at https://www.socialsecurity.gov/myaccount. If you see an error or attempted misuse of social security benefits, you can go to your local Social Security Office for assistance. Local offices can be found using the following office locator - https://secure.ssa.gov/ICON/main.jsp.

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, 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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents: The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For 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 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. We encourage you to 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.

For Rhode Island residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 0 Rhode Island residents impacted by this incident.