

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

HILARY HIGGINS
hhiggins@c-wlaw.com

JORDAN MORGAN
jmorgan@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

March 15, 2022

Via Email (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Security Breach Notification

To Whom It May Concern:

I serve as counsel for FM Expressions, located at 401 Taylor Ave, Gordonsville, VA 22942. We write to provide notification of a recent data security incident. By providing this notice, FM Expressions does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or about November 29, 2021, FM Expressions fell victim to a sophisticated ransomware attack. Upon discovery, FM Expressions immediately secured its network and engaged a third-party forensic firm to investigate the incident. After a thorough investigation, FM Expressions confirmed that a limited amount of personal information may have been impacted by this event.

On February 9, 2022, FM Expressions discovered that seven (7) residents of Maryland may have been affected by this incident. As our investigation is ongoing, we will provide supplemental notification should we determine additional residents of Maryland are potentially affected.

FM Expressions provided notice to the potentially impacted individuals via First Class Mail on March 15, 2022, and is offering the affected Maryland resident complimentary credit monitoring for 12 months. A copy of the draft notification letter is attached as ***Exhibit A***. The letter outlines the incident and provides potentially affected individuals with additional resources to protect their identity and monitor their credit history and personal accounts. FM Expressions is taking proactive steps to ensure that all state and federal notification obligations are complied with due to this incident.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

A handwritten signature in blue ink, appearing to read "Hilary Higgins", with a stylized flourish at the end.

Hilary Higgins, Esq.

Exhibit A



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

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

<<b2b_text_1(RE: Heading Variable Text-English)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

FM Expressions writes to notify you of a recent incident that may have involved your personal information described below.

FM Expressions takes the privacy of information in its care seriously, and while there is no evidence to suggest that any information was misused, in an abundance of caution, FM Expressions is providing you information about the incident, its response, and steps you can take to protect your information if you feel it is necessary to do so.

What Happened:

On or around November 29, 2021, FM Expressions experienced a network intrusion that affected a limited number of systems. Upon discovery, FM Expressions immediately engaged a third-party forensic firm to investigate the nature and scope of the incident. On February 9, 2022, FM Expressions discovered that a limited amount of information may have been accessed by an unauthorized party in connection with this incident.

At this time, there is no indication that any information has been misused. However, FM Expressions is providing this notification to you out of an abundance of caution and so that you may take steps to safeguard your information if you feel it is necessary to do so.

What Information Was Involved:

FM Expressions has no evidence that any information has been misused. The potentially accessed information may have included your first and last name, in combination with your <<b2b_text_3(Data Elements-English)>>.

What We Are Doing:

FM Expressions has taken steps to address the incident and is committed to protecting personal information in its care. Upon learning of this incident, FM Expressions immediately took steps to secure its systems, and to enhance the security of its network to prevent similar incidents from occurring in the future.

Credit Monitoring:

As a safeguard, we have arranged for you to enroll, at no cost to you, in identity monitoring services for 12 months. Due to privacy laws, we cannot register you directly. Additional information regarding how to activate the complimentary identity monitoring services is enclosed.

What You Can Do:

Sign up for Identity Monitoring Services – We encourage you to contact Kroll with any questions and to activate your free identity monitoring services at <https://enroll.krollmonitoring.com>, use your membership number, <<Membership Number s_n>>, and follow the steps to receive your identity monitoring service online within minutes. Please note the deadline to activate is <<b2b_text_6(Activation Deadline-English)>>. 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 describing your services is included with this letter. In addition to activating the complimentary identity monitoring service detailed within, FM Expressions recommends that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password and take additional steps to protect your account, and notify your financial institution or company if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your State Attorney General. Please review the additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to contact us at [1-888-653-0511](tel:1-888-653-0511), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time (excluding major U.S. holidays), or write us at 401 Taylor Ave, Gordonsville, VA 22942.

Sincerely,

W Scott White
CEO

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

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 will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud 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.

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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and 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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit 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 credit freeze 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and 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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) 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 by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>.