



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

May 10, 2022

Bruce A. Radke
312.463.6211
312.873-3763 Direct Fax
bradke@polsinelli.com

Via Electronic Mail – Idtheft@oag.state.md.us

Office of the Attorney General
Attn: Jeff Karberg, Administrator of the Identity Theft Program
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Security Incident

Dear Mr. Karberg,

We represent MX Holdings US, Inc., and its subsidiaries, including CFP Fire Protection, Inc., COSCO Fire Protection, Inc., Firetrol Protection Systems, Inc., and Flamex Inc. (together, “MX Holdings”) in connection with an incident that may have involved the personal information of one (1) Maryland resident and provide this notice on behalf of MX Holdings pursuant to MD. CODE ANN., COM. LAW § 14-3504(h). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While MX Holdings is notifying you of this incident, MX Holdings does not waive any rights or defenses relating to the incident or this notice, or the applicability of Maryland law on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

On or about October 28, 2021, MX Holdings discovered suspicious activity within its email system. MX Holdings immediately engaged a third-party cybersecurity firm to investigate the incident. The investigation determined that an unauthorized third party was able to temporarily access several email accounts. In response, MX Holdings retained a specialized document review vendor to examine the email accounts to determine whether any personal information was contained in the accounts.

NUMBER OF MARYLAND RESIDENTS AFFECTED

On or about April 5, 2022, MX Holdings determined that one (1) Maryland resident may have been involved in this incident. MX Holdings is notifying the Maryland resident of the incident by letter today, May 10, 2022. The notification letter will include an offer for twelve (12) months of complimentary credit monitoring and identity theft protection. Enclosed is a copy of the notice that is being sent to the Maryland resident via first-class United States mail.



Security Breach Notification
Maryland Attorney General's Office
May 10, 2022
Page 2

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, MX Holdings promptly prevented any further access to its system. MX Holdings is undertaking efforts to reduce the risk of a similar incident occurring in the future by implementing additional technical security measures and are continuing to explore methods to improve the security of all data in MX Holdings control. Finally, as discussed above, MX Holdings, is notifying the involved individual with complimentary credit monitoring and providing the individual with information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,

Bruce A. Radke

Enclosure

MX HOLDINGS US, INC.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

RE: NOTICE OF DATA BREACH

On behalf of MX Holdings US, Inc. and its subsidiaries, including CFP Fire Protection, Inc., COSCO Fire Protection, Inc., and Firetrol Protection Systems, Inc., we are writing to inform you of a recent incident that may have resulted in the temporary exposure of some of your personal information. We value the trust you place in our organization. We have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft. Nonetheless, we are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? On or about October 28, 2021, we observed suspicious activity within our email system. We immediately engaged a third-party forensic security firm to investigate the issue and confirm the security of our computer systems. This investigation determined that an unauthorized third party was able to temporarily access several email accounts. Additionally, we promptly retained a specialized document review vendor to examine the email accounts to determine whether any personal information was contained in the accounts.

What Information Was Involved? On or about April 5, 2022, we determined that the relevant email accounts contained certain personal information. That information varied by individual, but may have included your name, date of birth, Social Security number, driver's license number, passport number, financial account number, and/or limited medical information.

What We Are Doing. In addition to the actions described above, we have also taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. We are also notifying you of the incident so that you can be aware and take steps to protect yourself.

Finally, although we are not aware of any instances of fraud or identity theft resulting from this incident, in an abundance of caution, we are offering a complimentary one-year membership of *myTrueIdentity* online Credit Monitoring by TransUnion. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. *myTrueIdentity* online Credit Monitoring is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and *myTrueIdentity* online Credit Monitoring, including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. In addition to enrolling in the complimentary identity theft protection and credit monitoring service, you can find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call 844-571-2173 from 6:00 AM - 6:00 PM Pacific, Monday through Friday.

Sincerely,

Keith Fielding



1. Activation Code: <<Activation Code>>

1-Bureau TransUnion Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<12/24>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at **www.mytrueidentity.com** and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code

<<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<12/24>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *myTrueIdentity* online Credit Monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <http://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected <<RI Count>> Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any 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.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Washington, DC Residents: Washington, DC residents can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.