

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

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

An Important Message

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

This letter is to notify you of an incident involving a potential compromise of your personal information on the eFaucets.com website (“eFaucets.com”). eFaucets.com is operated by elmpovement, LLC (“elmpovement,” “we,” “us,” “our”). elmpovement takes the protection of customer information seriously, and while we have no direct evidence that your information was used by the attacker or others, out of an abundance of caution, we are contacting you directly to let you know what occurred, how elmpovement is responding and some precautionary measures you can take.

- **What Happened**

On February 3, 2020, elmpovement received a phone call from a customer who stated that they had experienced fraudulent activity on their credit card after shopping on eFaucets.com. This was confirmed a few days later by a report from VISA. We hired a top forensics consulting firm to assist with our ongoing investigation of this matter. They confirmed on February 10, 2020 that there had been an attack on eFaucets.com in which malicious scripts copied information entered on the checkout page, then shared the information with a domain named fontsawesomes.org. While the actual date of the breach cannot be confirmed, the investigation team discovered that fontsawesomes.org was registered on December 14, 2019.

- **What Information Was Involved**

The information that was vulnerable included name, address, e-mail address, phone number, full debit or credit card number, expiration date, and Card Verification Value (CVV) number. Username and password may have potentially been vulnerable to the extent they were used to checkout.

- **What We Are Doing**

Upon identifying this security concern, we immediately disabled use of all debit and credit cards on eFaucets.com. We also removed the offending scripts from our database. While we believe eFaucets.com can be made secure to resume debit and credit card transactions, we have made the business decision not to do so. Since early February eFaucets.com has not accepted any debit or credit card information. Currently we still offer customers the choice of using PayPal or placing their order over the phone. We have also reported this security incident to the FBI.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one (1) year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit [https://\[IDMonitoringURL\]](https://[IDMonitoringURL]) to activate and take advantage of your identity monitoring services.

You have until [\[Date\]](#) to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

- **What You Can Do**

The FTC and other consumer agencies provide information on steps consumers can take against potential misuse of personal data. As a precautionary measure, we recommend you remain vigilant by reviewing account statements and monitoring free credit reports, and take preventive actions, including those that are further detailed in Exhibit A attached to this letter.

- **For More Information**

We apologize for any inconvenience and concern that this may cause. Should you have any questions regarding this notice, including questions regarding your particular record, please do not hesitate to contact us:

By telephone: 1-???-???-???, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time

By mail: 8401 102nd Street, Suite 300

Pleasant Prairie, WI 53158

Sincerely,



Sean Hayes
General Manager

EXHIBIT A

IDENTITY THEFT PREVENTION INFORMATION

FTC and State Attorneys General Offices: You may take steps to protect yourself against potential misuse of data that has been the subject of a data security incident. The Federal Trade Commission discusses several steps, including obtaining and reviewing your credit report, filing a “fraud alert” and requesting a “credit freeze”. The most current and detailed information is available online (for answers to the questions below, see <https://www.ftc.gov/faq/consumer-protection>), but if you are not able to access the linked material, you may also contact the FTC by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, or by toll-free number, 1-877-FTC-HELP (382-4357) or 1-877-ID-THEFT (438-4338).

1. What are the steps I should take if I’m a victim of identity theft?
2. What is a fraud alert?
3. What is a credit freeze?
4. Should I apply for a new Social Security number?
5. What is an identity theft report?
6. What do I do if the police only take reports about identity theft over the Internet or telephone?
7. What do I do if the local police won’t take a report?
8. How do I prove that I’m an identity theft victim?

Fraud Alert and Security Freezes: A fraud alert tells creditors to take reasonable steps to verify your identity, including calling you before opening new accounts or changing your existing accounts. A fraud alert may be placed or removed at no cost to you. An initial fraud alert stays active for one year. To request a fraud alert, you will need to contact one of the following credit reporting agencies (see the FTC materials for further details). The credit reporting agency is required to notify the other two credit reporting agencies, who will also place a fraud alert on your credit file. You will then receive letters from all of them with instructions on how to obtain a free copy of your credit report from each.

Equifax Information Services, LLC
P.O. Box 105069
Atlanta, GA 30348
(800) 525-6285
www.equifax.com

Experian National Consumer Assistance
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022
1-800-680-7289
www.transunion.com

If you observe evidence of attempts to open fraudulent accounts and you have a copy of a police report reporting that you are experiencing identity theft, then you may also request a 7-year fraud alert. Be aware that placing a fraud alert does not always prevent new accounts from being opened or prevent a takeover of your existing accounts, so you should monitor any alerts sent to you by the credit monitoring companies. Also, be aware that a company may not be able to immediately extend credit to you if your identity can not be verified at the time you are applying for credit. You should consider providing a mobile telephone number when placing any fraud alert if you have one.

You also can contact the nationwide credit reporting agencies to place a security freeze to restrict access to your credit report altogether. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization.

However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing, or other services.

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
(800) 349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
(888) 397-3742

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022
(888) 909-8872

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;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have up to three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies 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 access to your credit report or to remove the security freeze altogether, 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 up to three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

Monitor Credit Reports and Accounts: When you receive your credit reports, you should look them over carefully and consider taking the steps recommended by the FTC. For example, look for accounts you did not open. Additionally, look for inquiries from creditors that you did not initiate. And finally, look for personal information that you do not recognize. Also, you should monitor your accounts for suspicious activity. If you see anything you do not understand, call the credit reporting agency or provider of your account at the telephone number on the credit report or account statements. If you do find suspicious activity on your credit reports, you may call your local police or sheriff's office and may be able to file a police report of identity theft and obtain a copy of the police report. Potentially, you may need to give copies of the police report to creditors to clear up your records. You may also make a report to the FTC.

Obtain Free Credit Reports: Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report regularly for at least the next one to two years. Each of the three credit reporting agencies is required to provide you with a free credit report, at your request, once every 12 months. You may visit www.annualcreditreport.com, the only Web site authorized by Equifax, Experian and TransUnion for this purpose, to find out more. This website also provides instructions for making a request by phone (1-877-322-8228) or by mailing a request on a form supplied at the site and sending it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ 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 can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ 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.