

September 24, 2024

Via Email: IDtheft@oag.state.md.us

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

To Whom it May Concern:

This letter serves as notice that McArthurGlen Europe Inc. ("MGE") experienced a data security incident. Specifically, in late July 2024, MGE discovered and confirmed that system files and information were accessed and exported by an unknown threat actor. MGE moved quickly to contain the intrusion. MGE also investigated the incident and notified federal law enforcement. A general description of the incident and the remedial measures taken are provided in the attached notice sent to the 22 affected Maryland residents.

Your office is welcome to contact me at daniel.raymond@arnoldporter.com or (312) 583-2379 if you require additional information.

Sincerely,



Daniel Raymond
Senior Associate
Arnold & Porter LLP
70 West Madison Street
Suite 4200
Chicago, Illinois 60602-4231

Attachment

McArthurGlen Europe Inc.
6400 Georgetown Pike
McLean, VA 22101
(703)880-2299

September __, 2024

[Individual's name]
[Individual's address]
[City, State, Zip]

Notice of Data Breach

Dear _____:

McArthurGlen Europe Inc. takes the protection of your personal information very seriously. Regrettably, we write to inform you of an incident that involved some of that information belonging to McArthurGlen Europe Inc., Europe Trust, and Joseph W. Kaempfer, Jr. (together, collectively, "MGE"). Please read this notice carefully, as it provides information about the incident, the personal information that may have been involved, the steps we have taken to ensure the security of our systems, and the resources available to you to protect yourself against any unauthorized use of your personal information. We have included our contact details below should you need any further information.

What Happened?

In late July 2024, MGE experienced a cyberattack on parts of our network. As a result, there is reason to believe that sensitive information belonging to certain individuals affiliated with MGE, including certain employees and investors, was compromised. We have been working in close collaboration with external cyber forensics experts and the appropriate authorities to thoroughly investigate the incident and secure our systems.

What Information Was Involved?

You are receiving this notice because our review determined that the cyberattack may have resulted in unauthorized access and acquisition of one or more files containing your name, Social Security number, driver's license number, passport number, and login credentials enabling access to online accounts. The fact that you are receiving this notice does not mean that all or more than one of the aforementioned files and information relating to your personal information were actually acquired.

What We Are Doing

Because the protection of your privacy is so important to us, we have taken several steps to further fortify our systems and detect suspicious activity on our networks. And while we have no indication that your information has been used to commit fraud or identity theft, we are offering you a complimentary two-year membership of Experian's® IdentityWorks.SM This product provides you with full-service identity detection and resolution of identity theft.

To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: [enrollment end date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: [code]

If you have questions about the product or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 890-9332 by [insert enrollment end date]. Be prepared to provide engagement number [insert] as proof of eligibility for the identity restoration services by Experian.

What You Can Do

We encourage you to remain vigilant for incidents of fraud and identity theft by carefully reviewing your payment cards and personal accounts for unauthorized charges and be sure to monitor free credit reports for fraudulent or unusual activity.

If you suspect an unauthorized charge has been placed on your account, report it to your payment card issuer immediately. According to the payment card brands' policies, you are not responsible for unauthorized charges to your account if you report them in a timely manner.

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

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

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

For More Information

If you have additional questions, please mail us a letter at McArthur Glen Europe Inc., 6400 Georgetown Pike, McLean, VA 22101, or call our general company phone line at 703-880-2299.

Sincerely,



Lisa Sarrge
Vice President and Treasurer
McArthur Glen Europe Inc.

ADDITIONAL DETAILS REGARDING YOUR 2-YEAR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (877) 890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 2 years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. You should obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission and your state attorney general are as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For Connecticut residents: *Connecticut Office of the Attorney General*, 165 Capitol Avenue, Hartford, CT, 06106, <https://portal.ct.gov/ag>

For DC residents: *District of Columbia Office of the Attorney General*, 400 6th Street NW, Washington, DC 20001, 202-727-3400, <https://oag.dc.gov/>

For Maryland residents: *Maryland Office of the Attorney General*, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For New York residents: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583/1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *State of New York Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 800-771-7755, <https://ag.ny.gov/>

For Virginia residents: *Virginia Office of the Attorney General*, 202 North Ninth Street, Richmond, Virginia 23219, 804-786-2071, <https://www.oag.state.va.us>

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, please contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit

bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If a creditor can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, please contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com

TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You will need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save time by lifting the freeze only at that particular credit bureau. Otherwise, you will need to make the request with all three credit bureaus.