FOLEY
FOLEY & LARDNER LLP

ATTORNEYS AT LAW
321 NORTH CLARK STREET, SUITE 3000
CHICAGO, IL 60654-4762
312.832.4500 TEL
312.832.4700 FAX
WWW.FOLEY.COM

WRITER'S DIRECT LINE
312.832.4367
atantleff@foley.com

CLIENT/MATTER NUMBER
650145-0024

August 14, 2024

VIA E-MAIL: Idtheft@oag.state.md.us

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

Re: Notification Pursuant to Md. Code Com. Law § 14-3501 *et seq.*

Dear Attorney General Brown:

We are writing on behalf of our client, Enterprise Financial Group, Inc. ("EFG"), to notify you of a security incident involving the personal information of approximately two hundred and twenty-six (226) Maryland residents.

NATURE OF THE UNAUTHORIZED DISCLOSURE

On February 18, 2024, EFG became aware of a security incident impacting its internal systems. Upon discovering the issue, EFG took immediate steps to investigate, contain, and eradicate the incident. EFG also commenced an investigation with the assistance of external cybersecurity experts to determine the nature and scope of the incident. Based on the investigation, EFG determined that an unauthorized third party accessed and copied files contained within certain segments of its network on February 18, 2014. The investigation confirmed that this incident occurred due to unknown vulnerabilities affecting EFG's third-party VPN appliance, despite EFG's proactive efforts to promptly address and patch all vulnerabilities reported by the third-party provider. EFG has since implemented all available patches.

As part of its investigation, EFG retained external specialists to conduct an extensive manual review to identify whether personal information belonging to individuals may have been present in the files that were affected during the incident. Based on that review, which concluded on July 15, 2024, EFG confirmed that the information involved in this incident included some combination of the Maryland residents' names, addresses, Social Security numbers, driver's license numbers, bank account or payment card numbers, tax ID numbers, and medical information. Not all data elements were present for the entire population of affected individuals.

STEPS TAKEN RELATED TO THE INCIDENT

To date, EFG is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, on August 14, 2024, EFG mailed written notification to the affected Maryland residents. Enclosed is a template copy of the notification letter. EFG is providing the residents whose Social Security numbers may have been affected with 12 months of credit monitoring at no charge and has established a dedicated toll-free support line that is staffed to answer any questions individuals may have about the incident or the services available to them. Within the letter, EFG also advises the affected residents on general best practices and safeguards to protect themselves from identity theft, including to always remain vigilant in reviewing account statements and credit reports for unauthorized activity on a regular basis, as well as the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports.

At EFG, protecting the privacy of personal information is a top priority. EFG remains fully committed to maintaining the privacy of personal information in its possession and has taken numerous precautions to safeguard it. EFG has addressed and fixed the vulnerabilities and implemented additional security measures throughout its environment. EFG continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any inquiries concerning this notification, please do not hesitate to contact me.

Sincerely,

Aaron K. Tantleff
Foley & Lardner LLP

Enclosure: Sample Notification Letter

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

[redacted]

[redacted]

Dear [redacted]:

At Enterprise Financial Group Inc. ("EFG"), we value and respect the privacy of your information. We are writing to let you know about a recent security incident that may have involved some of your personal information. This letter contains information about what happened, the measures taken in response, and steps you can take to help protect your information.

WHAT HAPPENED?

On February 18, 2024, we became aware of a security incident impacting our internal systems and took immediate steps to investigate, contain, and eradicate the incident with the assistance of external cybersecurity experts. The investigation determined that an unauthorized third party accessed and copied files contained within certain segments of our network on February 18, 2024. Our investigation confirmed that this incident occurred due to unknown vulnerabilities affecting our third-party VPN appliance, despite our proactive efforts to promptly address and patch all vulnerabilities reported by the third-party provider. We have since implemented all available patches and continue to work closely with the third-party provider to mitigate any future risks.

As part of this investigation, we initiated a detailed review, which concluded on July 15, 2024, to identify whether personal information belonging to individuals may have been present in the files that were affected during the incident.

WHAT INFORMATION WAS INVOLVED?

Our review determined that the files copied from our environment contained at least one piece of your personal information, such as your full name, Social Security number, driver's license number, passport number, bank account or payment card numbers, medical information, and/or insurance information.

WHAT WE ARE DOING.

Upon learning of the security incident, we immediately implemented our incident response protocol, which included working closely with external cybersecurity experts to investigate, contain, and eradicate the incident, as well as to confirm the security of our network environment. We have remediated the vulnerability by applying a patch provided by the third-party VPN provider and enhanced security measures to help protect the privacy of information stored on our systems. Additionally, we fully replaced the third-party VPN appliance as a precaution to prevent further potential disclosures of information.

Although we have no evidence to suggest that your information has been or will be misused, we are notifying you out of an abundance of caution. To help address any concerns you may have, we have arranged for you to enroll, at no cost to you, in comprehensive credit monitoring and identity protection services for [redacted] through Equifax®, one of the three nationwide credit reporting companies. A description of this service and instructions on how to enroll can be found within the enclosed "Other Important Information" document included with this letter.

WHAT YOU CAN DO.

Please review the enclosed "Other Important Information" document included with this letter for further steps you can take to protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. It is also recommended that you remain vigilant by reviewing your account statements and monitoring your credit reports for unauthorized activity. If you discover any suspicious or unusual activity on your accounts, you should promptly notify the financial institution or company with which your account is maintained.

FOR MORE INFORMATION.

For further information and assistance, please contact our dedicated incident response line at [redacted] between 8 a.m. – 8 p.m. Central Time, Monday through Friday.

Sincerely,
Jennifer A. Rappaport
President & CEO
Enterprise Financial Group Inc.

OTHER IMPORTANT INFORMATION

Enrolling in Complimentary Credit Monitoring.

[redacted]

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of [redacted] then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the nationwide credit reporting agencies. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's (FTC) website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the national credit reporting agencies for the purpose of requesting a copy of your credit report and other general inquiries is provided below:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213
- **Innovis**, PO Box 530088, Atlanta, GA 30353-0088, www.innovis.com, 1-800-540-2505

Fraud Alert. You have the right to place an initial or extended "fraud alert" on your file at no cost by contacting any of the nationwide credit reporting agencies. Contact information for the national credit reporting agencies for the purposes of placing a fraud alert on your file is provided below. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. For this reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for 7 years, on your credit file.

- **Equifax**, PO Box 105069, Atlanta, GA 30348-5069, www.equifax.com/personal/credit-report-services/credit-fraud-alerts, 1-800-525-6285
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html, 1-888-397-3742
- **TransUnion**, P.O. Box 160, Woodlyn, PA 19094, www.transunion.com/fraud-alerts, 1-800-916-8800
- **Innovis Consumer Assistance**, PO Box 530088 Atlanta, GA 30353-0088, https://www.innovis.com/personal/fraudActiveDutyAlerts, 1-866-712-0021

Security Freeze. You have the right to place, lift, or remove a "security freeze" on your credit report, free of charge. 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, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze separately with each of the consumer reporting agencies. To place a security freeze on your credit report, you may do so by contacting each of the consumer reporting agencies through the contact information below:

- **Equifax**, PO Box 105788, Atlanta, GA 30348-5788, www.equifax.com/personal/credit-report-services/credit-freeze, 1-800-298-0045
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html, 1-888-397-3742
- **TransUnion**, PO Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze, 1-888-909-8872
- **Innovis**, PO Box 530088 Atlanta, GA 30353-0088, www.innovis.com/personal/securityFreeze, 1-866-712-4546

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. 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.

The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or up to 3 business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and may 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. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity 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 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the credit bureaus 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. The credit bureaus have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to remove the security freeze.

Federal Trade Commission and State Attorneys General Offices. 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 FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (438-4338). This notice has not been delayed by law enforcement.

- **For Iowa Residents**: You are advised to report suspected incidents of identity theft to law enforcement or the Iowa Attorney General's Office at Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 1- 515-281-5926 or 1-888-777-4590.
- **For Maryland Residents**: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, Telephone: 1-410-576-6491 or 1-888-743-0023.
- **For New Mexico Residents**: You have rights pursuant to the Fair Credit Reporting Act ("FCRA"), 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 FCRA, 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 FCRA not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-_fcra.pdf, or by writing Consumer Response 30-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.
- **For New York Residents**: You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General at https://ag.ny.gov/ or by calling 1-800-771-7755; the New York State Police at http://troopers.ny.gov/ or by calling 1-518-457-6721; and/or the New York Department of State at https://www.dos.ny.gov or by calling 1-800-697-1220.
- **For North Carolina Residents**: You may obtain additional information about preventing identity theft provided by the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/identity-theft/, by calling 1-877- 566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.
- **For Oregon Residents**: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

- **For District of Columbia Residents**: You may obtain additional information about identity theft prevention and protection from the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, https://oag.dc.gov.